FortiClient v5.0 Patch Release 5
XML Reference

FortiClient v5.0 Patch Release 5 XML Reference

September 11, 2013

04-505-185162-20130911

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2012-11-23	Initial release.
2013-01-04	Updated for FortiClient v5.0 Patch Release 1.
2013-04-02	Updated for FortiClient v5.0 Patch Release 2.
2013-06-17	Updated for FortiClient v5.0 Patch Release 4.
2013-08-19	Updated for FortiClient v5.0 Patch Release 5.
2013-09-11	Description for <localid> tag.

Introduction

FortiClient has been completely re-designed for v5.0. FortiClient provides a comprehensive network security solution for endpoints while improving your visibility and control. FortiClient allows you to manage the security of multiple endpoint devices from the FortiGate interface. This document provides an overview of FortiClient v5.0 Patch Release 5 XML configuration.

This document was written for FortiClient (Windows) v5.0 Patch Release 5. Not all features described in this document are supported for FortiClient (Mac OS X) v5.0 Patch Release 5.

For more information on FortiClient installation and configuration, refer to the FortiClient v5.0 Patch Release 5 Administration Guide available at www.FortiClient.com or at the Fortinet Technical Documentation web site http://docs.fortinet.com.

This document includes the following chapters:

- XML Configuration File
- Example XML Configurations
- Backup or Restore the Configuration File
- Advanced Features

XML Configuration File

FortiClient configuration

File structure

FortiClient supports importation and exportation of its configuration via an XML file. This section defines and describes the format of that file.

File extensions

FortiClient supports the following four file types:

- .conf

  A plain-text configuration file.
- .sconf

  A secure (encrypted) configuration file.
- .conn

  A plain-text VPN connection configuration file.
- .sconn

  A secure (encrypted) VPN connection configuration file.

A configuration file can be generated from the settings page of FortiClient dashboard or by using the command-line program: FCConfig.exe, installed with FortiClient. See “Backup or Restore the Configuration File” on page 97 for more information.

Configuration file sections

The configuration file contains the following major sections:

- Meta data

  Basic data controlling the entire configuration file.
- System Settings

  General configurations that is not specific to any of the modules listed below (or affects more than one module).
- VPN
- Certificates
- Antivirus
- Endpoint Control
- Single Sign-On Mobility Agent
- WAN Optimization
- Web Filtering
- Application Firewall
- Vulnerability Scan

Encrypted username and password

Several tag elements are named <password>. All such tags are always encrypted during configuration exports. For modified and imported configurations, FortiClient accepts either encrypted or plain-text passwords.

Here is an example of an encrypted password tag element. The password starts with *Enc*:

```
<password>Enc9b4e1aae22c65e638aed4e47fbd225256a3b7a24b53f8370d6bc3b9
    aa90cecd5086c995f0549e944b4acc951e4844529c71d81280de2b951</pass
    word>
```

Several <username> tags also follow this format.

IP addresses

IP address tag elements usually refer to IP version 4 addresses (IPv4). A fully qualified domain name (FQDN) may also be provided. Here are two examples:

- Single IP: 74.196.82.243
- FQDN: www.fortinet.com

Boolean values

Elements that determine if a feature is enabled or disabled use Boolean values. The configuration file accepts 0 for false and 1 for true.

Meta data

All of the XML tags and data in a configuration file are contained inside the tag <forticlient_configuration>. An empty configuration file will look like this:

```
<?xml version="1.0" encoding="utf-8"?>
<forticlient_configuration>
</forticlient_configuration>
```

The first line of the file includes an XML version number as well as the encoding. This is the standard XML start tag.

The following meta data is supported:

```
<forticlient_version>5.0.5.308</forticlient_version>
```

FortiClient version number if the file is exported from FortiClient.

```
<version>5.0</version>
```

Version of the configuration file.

```
<date>2013/08/08</date>
```

Date when the file was generated.

```
<partial_configuration>0</partial_configuration>
```

A flag that controls whether the configuration will be replaced or added in import/restore. Possible values are 0 or 1.

```
<os_version>windows</os_version>
```

Indicates whether this configuration is generated from Microsoft Windows or Mac OS X. Possible values are `windows` or `mac`.

System Settings

System settings are contained inside the <system></system> tags. It includes the following subsections:

- UI settings
- Log settings
- Proxy settings
- Update settings

UI settings

UI related information are contained inside the <ui></ui> tags:

```
<forticlient_configuration>
  <system>
    <ui>
      <ads>1</ads>
      <default_tab>AV</default_tab>
      <flashing_system_tray_icon>1</flashing_system_tray_icon>
      <hide_system_tray_icon>0</hide_system_tray_icon>
      <suppress_admin_prompt>0</suppress_admin_prompt>
      <password>Enc9b4e1aae22c65e638aed4e47fbd225256a3b7a24b53f8370
          d6bc3b9aa90cecd5086c995f0549e944b4acc951e4844529c71d8128
          0de2b951</password>
      <culture-code>en-us</culture-code>
      <show_passcode>0</show_passcode>
      <gpu_rendering>0</gpu_rendering>
    </ui>
  </system>
</forticlient_configuration>
```

The following table provides UI setting XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<ads>	Enable or disable advertisements. Boolean value: [0 | 1]	1
<default_tab>	The tab selected by default on dashboard. Select one of the following: • AV: Antivirus • WF: Parental Control/Web Filtering • FW: Application Firewall • VPN: Remote Access • VULN: Vulnerability Scan	AV

<flashing_system_tray_icon>	The system tray flashes while FortiClient background processes are running. Boolean value: [0 | 1]	1
<hide_system_tray_icon>	Hide the system tray icon. Boolean value: [0 | 1]	0
<suppress_admin_prompt>	Do not ask for an administrator password for tasks that require super_user permission to complete. Boolean value: [0 | 1]	0
<password>	Either encrypted or non-encrypted password. For more information, see “Encrypted username and password” on page 8.	
<culture-code>	The localized language used by the FortiClient dashboard. Select one of the following: • de-de: German • en-us: English (United States) • es-es: Spanish (Spain) • fr-fr: French (France) • ja-jp: Japanese • pt-br: Portuguese (Brazil) • kr-kr: Korean • zh-cn: Chinese (Simplified) • zh-tw: Chinese (Traditional)	en-us
<show_passcode>	Display *Passcode* instead of *Password* in the VPN tab on the FortiClient console. Boolean value: [0 | 1]	0
<gpu_rendering>	Enable or disable GPU rendering. Boolean value: [0 | 1]	0

Log settings

Log-related information will be inside the <log_settings></log_settings> tags:

```
<forticlient_configuration>
  <system>
    <log_settings>
      <level>6</level>
      <!--0=emergency, 1=alert, 2=critical, 3=error, 4=warning,
          5=notice, 6=info, 7=debug, -->
      <log_events>ipsecvpn,sslvpn,scheduler,firewall,av,clientmanag
          er,proxy,shield,webfilter,endpoint,fssoma,wanacc,configd
          ,vuln</log_events>
      <!--ipsecvpn=ipsec vpn, sslvpn=ssl vpn, firewall=firewall,
          av=antivirus, webfilter=webfilter, vuln=vulnerability
          scan, wanacc=wan acceleration, fssoma=single sign-on
          mobility for fortiauthenticator, scheduler=scheduler,
          update=update, proxy=fortiproxy, shield=fortishield,
          endpoint=endpoint control, configd=configuration, -->
      <remote_logging>
        <log_upload_enabled>0</log_upload_enabled>
        <log_upload_server />
        <log_upload_ssl_enabled>1</log_upload_ssl_enabled>
        <log_retention_days>90</log_retention_days>
        <netlog_categories>7</netlog_categories>
        <log_upload_freq_hours>1</log_upload_freq_hours>
        <log_last_upload_date>0</log_last_upload_date>
      </remote_logging>
    </log_settings>
  </system>
</forticlient_configuration>
```

The following table provides log settings XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<level>	Select the level of logging. Select one of the following: • 0: emergency • 1: alert • 2: critical • 3: error • 4: warning • 5: notice • 6: information • 7: debug	6

<log_events>	FortiClient events or processes to log. One or more comma-separated list of: • ipsecvpn: IPsec VPN • sslvpn: SSL VPN • firewall: Firewall • av: Antivirus • webfilter: Web Filtering • vuln: Vulnerability Scan • wanacc: WAN Optimization • fssoma: Single Sign-On (SSO) mobility agent for FortiAuthenticator • scheduler: Scheduler • update: Update • proxy: FortiProxy • shield: FortiShield • endpoint: Endpoint Control • configd: Configuration	ipsecvpn,sslvpn,scheduler,update,firewall,av,clientmanager,proxy,shield,webfilter,endpoint,fssoma,wanacc,configd,vuln (enable all events by default)
<remote_logging> elements		
<log_upload_enabled>	Upload FortiClient logs to the FortiGate. Boolean value: [0 | 1]	0
<log_upload_server>	IP address of the FortiAnalyzer/FortiManager to send logs to.	
<log_upload_ssl_enabled>	Enable or disable use of SSL protocol during log upload. Boolean value: [0 | 1]	1
<log_retention_days>	If the server is not reachable, the number of days to retain the logs before being deleted.	90
<netlog_categories>	Type of logs to upload. Bitmask: 1 = traffic logs 2 = vulnerability logs 4 = event logs Since these are bitmasks, you may combine as follows: 3 = 1 or 2 (traffic and vulnerability) 5 = 1 or 4 (traffic and event) 6 = 2 or 4 (vulnerability and event) 7 = 1 or 2 or 4 (all logs)	7

<log_upload_freq_hours>	Upload frequency interval in hours	1
<log_last_upload_date>	Date of the most recent log upload.	

The FortiShield daemon protects FortiClient's own filesystem and registry settings from modification by unauthorized persons.

Proxy settings

Proxy-related information are contained inside the <proxy></proxy> tags:

```
<forticlient_configuration>
  <system>
    <proxy>
      <update>0</update>
      <online_scep>0</online_scep>
      <virus_submission>0</virus_submission>
      <type>http</type>
      <address />
      <port>80</port>
      <username>Encb33db9a4dd1786a5f9b6209d13a65d160f14e0d980748703
          </username>
      <password>Enccfd104974578a3067d14a16c1790466d94b3f72197b693aa
          </password>
    </proxy>
  </system>
</forticlient_configuration>
```

The following table provides proxy setting XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<update>	Enable or disable updates. Boolean value: [0 | 1]	0
<online_scep>	Enable or disable Simple Certificate Enrollment Protocol (SCEP). Enable this option if you use SCEP and to access it and you have to go through a proxy. Boolean value: [0 | 1]	0
<virus_submission>	Enable or disable virus submission to FortiGuard (FDN). Boolean value: [0 | 1]	0

<type>	Select one of the following: • HTTP • SOCKS4 • SOCKS5	HTTP
<address/>	IP address or FQDN.	
<port>	Port number. Port range: 1 to 65535	80
<username>	Either encrypted or non-encrypted user name. For more information, see "Encrypted username and password" on page 8.	
<password>	Either encrypted or non-encrypted password. For more information, see "Encrypted username and password" on page 8.	

Update settings

Update-related information is contained inside the <update></update> tags:

```
<forticlient_configuration>
  <system>
    <update>
      <use_custom_server>0</use_custom_server>
      <server />
      <port>80</port>
      <fail_over_servers>server1.fortinet.com:8008;172.81.30.6:80;s
          erver2.fortinet.com:80</fail_over_servers>
      <timeout>60</timeout>
      <failoverport>8000</failoverport>
      <fail_over_to_fdn>1</fail_over_to_fdn>
      <update_action>notify_only</update_action>
      <scheduled_update>
        <enabled>1</enabled>
        <type>interval</type>
        <daily_at>03:00</daily_at>
        <update_interval_in_hours>3</update_interval_in_hours>
      </scheduled_update>
    </update>
  </system>
</forticlient_configuration>
```

The following table provides update setting XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<use_custom_server>	Define a custom server for updates. Boolean value: [0 | 1]	0

<server>	IP address or FQDN of the update server.	
<port>	Port number of the update server. Port range: 1 to 65535	80
<fail_over_servers>	Update servers to try if the primary server could not be reached. Separate multiple servers with a semicolon. IP address or FQDN, followed by a colon and the port number if applicable.	
<timeout>	Connection timeout, in seconds, when attempting to reach a custom update server.	60
<failoverport>	Failover port number. Port range: 1 to 65535	8000
<fail_over_to_fdn>	Determines whether or not to use FortiGuard servers if communication with custom <server> fails.	1
<update_action>	Select one of the following: • download_and_install • download_only • notify_only	notify_only
<scheduled_update> tags		
<enabled>	Enable or disable scheduled updates. Boolean value: [0 | 1]	1
<type>	Update frequency: daily or at regular intervals. Select one of the following: • daily • interval	interval
<daily_at>	Time of the day, in the format HH:MM, this field is mandatory if the <type> tag is set to daily.	
<update_interval_in_hours>	Update interval in hours if the <type> tag is set to interval.	3

When <use_custom_server> is 0 or both <server> and <fail_over_servers> are each an empty (NULL) string, FortiClient will only use the default FortiGuard server for software updates. If a string is specified in <server> and communication fails with that server, each of the servers specified in <fail_over_servers> are tried until one succeeds. If that also fails, then software updates will not be possible unless <fail_over_to_fdn> is set to 1.

If communication fails with the server(s) specified in both <server> and <fail_over_servers>, <fail_over_to_fdn> determines the next course of action as listed below:

<server>	<fail_over_to_fdn>	Result
"" (empty strings)	0	Only FortiGuard server is used.
"" (empty strings)	1	Only FortiGuard server is used.
"xyz" (valid IP address)	0	FortiGuard server is never used.
"xyz" (valid IP address)	1	FortiGuard server is used only as failover.

FortiProxy settings

FortiProxy information is contained inside the <fortiproxy></fortiproxy> tags:

```
<forticlient_configuration>
  <system>
    <fortiproxy>
      <enabled>1</enabled>
      <enable_https_proxy>1</enable_https_proxy>
      <http_timeout>60000</http_timeout>
      <client_comforting>
        <pop3_client>1</pop3_client>
        <pop3_server>1</pop3_server>
        <smtp>1</smtp>
      </client_comforting>
      <selftest>
        <enabled>0</enabled>
        <last_port>-172</last_port>
        <notify>0</notify>
      </selftest>
    </fortiproxy>
  </system>
</forticlient_configuration>
```

The following table provides FortiProxy XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<enabled>	Enable or disable FortiProxy. Boolean value: [0 | 1]	1
<enable_https_proxy>	Enable or disable HTTPS proxy. Boolean value: [0 | 1]	1

<http_timeout>	Connection timeout in milliseconds (ms).	60000
<client_comforting> elements		
<pop3_client>	POP3 client comforting. Client comforting helps to prevent POP3 clients from complaining that the server has not responded in time. Boolean value: [0 | 1]	1
<pop3_server>	POP3 server comforting. Server comforting helps to prevent POP3 servers from complaining that the client has not responded in time. Boolean value: [0 | 1]	1
<smtp>	SMTP comforting. SMTP comforting helps to prevent SMTP clients from complaining that the server has not responded in time. Boolean value: [0 | 1]	1
<selftest> elements		
<enabled>	Enable or disable self tests. FortiProxy periodically checks its own connectivity to determine if it is able to proxy other applications traffic. Boolean value: [0 | 1]	1
<last_port>	Last port number used. This is the highest port number you want to allow FortiProxy to listen on. Use to prevent FortiProxy from binding to another port that another service normally uses.	65535
<notify>	Notify the user if self-tests fail. Boolean value: [0 | 1]	1

VPN

VPN related information is contained inside the <VPN></VPN> tags. The VPN configuration includes the following subsections:

- VPN options

  Global options that apply to both SSL VPN and IPsec VPN.
- SSL VPN

  SSL VPN related configurations.
- IPsec VPN

  IPsec VPN configurations.

IPsec VPN and SSL VPN each have two subsections:

- Options
  Options related to the specific type of VPN.
- Connections
  User defined connections.

VPN options

The VPN <options> tag contains global information controlling VPN states:

```
<forticlient_configuration>
  <vpn>
    <options>
      <current_connection_name>ssldemo</current_connection_name>
      <current_connection_type>ssl</current_connection_type>
      <save_password>0</save_password>
      <autoconnect_tunnel />
      <keep_running_max_tries>0</keep_running_max_tries>
      <minimize_window_on_connect>1</minimize_window_on_connect>
      <allow_personal_vpns>1</allow_personal_vpns>
      <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
      <show_vpn_before_logon>0</show_vpn_before_logon>
      <use_windows_credentials>1</use_windows_credentials>
      <show_negotiation_wnd>0</show_negotiation_wnd>
    </options>
  </vpn>
</forticlient_configuration>
```

The following table provides VPN option XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
`<current_connection_name>`	Name of the current connection, if any.	
`<current_connection_type>`	Type of the current connection. Select either: `[ipsec | ssl]`	
`<autoconnect_tunnel>`	Name of the configured IPsec VPN or SSL VPN tunnel to automatically connect to when FortiClient starts. Requires that the `<save_password>` tag be set to 1.	
`<keep_running_max_tries>`	The maximum number of attempts to make when retrying a VPN connection that was lost due to network issues. If this tag is set to 0, it will retry indefinitely.	`0`
`<save_password>`	Save user provided connection passwords. Boolean value: `[0 | 1]`	`0`

<minimize_window_on_connect>	Minimize the FortiClient dashboard after successfully establishing a connection. Boolean value: [0 | 1]	1
<allow_personal_vpns>	Enable end users to create, modify, and use personal VPN configurations. Boolean value: [0 | 1]	1
<use_legacy_vpn_before_logon>	Use the old VPN before logon interface. Boolean value: [0 | 1]	1
<show_vpn_before_logon>	Allow user to select VPN connection from a list before login onto the system. Boolean value: [0 | 1]	0
<use_windows_credentials>	Connect with current user name and password. Boolean value: [0 | 1]	1
<show_negotiation_wnd>	Display information on FortiClient dashboard while establishing connections. Boolean value: [0 | 1]	0

SSL VPN

SSL VPN configurations consist of one options section, followed by one or more connection details.

```
<forticlient_configuration>
<vpn>
  <sslvpn>
    <options>
      <enabled>1</enabled>
      <keep_connection_alive>1</keep_connection_alive>
    </options>
    <connections>
      <connection>
        <name>ssldemo</name>
        <description>Texas Office SSL VPN</description>
        <server>ssldemo.fortinet.com:10443</server>
        <username>Enc6bd50fbb0aec8c122142e572d107bfc10492cd61754bb
            45308d66c7cb0
        </username>
        <single_user_mode>0</single_user_mode>
        <ui>
          <show_remember_password>1</show_remember_password>
          <show_alwaysup>1</show_alwaysup>
          <show_autoconnect>1</show_autoconnect>
        </ui>
        <password>Encca7f0c3676ddaaf9685f4cd71e399b80bfa86795c556e
            4413cb9e14b12
```

```
            </password>
            <certificate />
            <warn_invalid_server_certificate>1</warn_invalid_server_ce
                rtificate>
            <prompt_certificate>0</prompt_certificate>
            <prompt_username>0</prompt_username>
            <on_connect>
              <script>
                <os>windows</os>
                <script>
                  <script>
                  <![CDATA[
                  net use x: \\server1\share /user:#username#
                       #password#
                  net use y: \\server2\share /user:#username#
                       #password#
                  net use z: \\server3\share /user:#username#
                       #password#
                  copy %temp%\*.logs z:\share\logs\
                  copy z:\files\*.* c:\files\
                  ]]>
                </script>
              </script>
            </on_connect>
            <on_disconnect>
              <script>
                <os>windows</os>
                <script>
                  <script>
                    <![CDATA[
                    net use x: /DELETE
                    net use y: /DELETE
                    net use z: /DELETE
                    ]]>
                  </script>
                </script>
              </script>
            </on_disconnect>
          </connection>
        </connections>
        </sslvpn>
      </vpn>
      </forticlient_configuration>
```

The following table provides SSL VPN XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<sslvpn> <options> elements		
<enabled>	Enable or disable SSL VPN. Boolean value: [0 | 1]	1
<keep_connection_alive>	Retry restoring connection of an active VPN session. Boolean value: [0 | 1]	

The <connections> tag may contain one or more <connection> elements. Each <connection> has the following:

- information used to establish an SSL VPN connection
- on_connect: a script to run right after a successful connection
- on_disconnect: a script to run just after a disconnection

Connection details is described in table below.

The following table provides VPN connection XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<name>	VPN connection name.	
<description>	Optional description to identify the VPN connection.	
<server>	IP address or FQDN of SSL server, along with the port number as applicable.	Default port number: 443
<username>	Either encrypted or non-encrypted user name on SSL server. For more information, see "Encrypted username and password" on page 8.	
<single_user_mode>	Enable or disable single user mode. If enabled, new and existing VPN connections cannot be established or will be disconnected if more than one user is logged in. Boolean value: [0 | 1]	0
<password>	Either encrypted or non-encrypted password of the given user	
<certificate>	Encrypted certificate name to connect with.	
<warn_invalid_server_certificate>	Enable or disable displaying of a warning message if the server certificate is invalid. Boolean value: [0 | 1]	0

<prompt_certificate>	Request for a certificate during a connection establishment. Boolean value: [0 | 1]	0
<prompt_username>	Request for a user name. Boolean value: [0 | 1]	1
<ui> elements		
<show_remember_password>	Display the remember passwords checkbox in the console. Boolean value: [0 | 1]	
<show_alwaysup>	Display the always up checkbox in the console. Boolean value: [0 | 1]	
<show_autoconnect>	Display the autoconnect checkbox in the console. Boolean value: [0 | 1]	

The elements of the <ui> tag are set by the FortiGate following an SSL VPN connection.

VPN connection name is mandatory. If a connection of this type and this name exists, its values will be overwritten with the new ones.

The <on_connect> and <on_disconnect> tags both have very similar tag structure:

```
<on_connect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
        ]]>
      </script>
    </script>
  </script>
</on_connect>
<on_disconnect>
  <script>
    <os>windows</os>
    <script>
      <script>
```

```
            <![CDATA[
            ]]>
          </script>
        </script>
      </script>
    </on_disconnect>
```

The following table provides CDATA XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
`<os>`	The operating system for which the script is written. Select either: `[windows | mac]`	
`<script>`	The MS DOS batch or Mac OS X shell script to run.	
`<![CDATA[` `]]>`	Wraps the scripts in CDATA elements.	

The DOS batch or Mac OS X Shell script should be wrapped inside the CDATA tag, one line per command, just like a regular script file.

The script will be executed in the context of the user that connected the tunnel. Wherever #username# is used in the script, it will be automatically substituted with the xauth username of the user that connected the tunnel. Where `#password#` is used in the script, it will be automatically substituted with the xauth password of the user that connected the tunnel. The XML file should have carriage returns and line feeds as appropriate.

The example scripts above show a script that mounts several network drives after an SSL connection is established. The drives are unmounted with the corresponding scripts in the `<on_disconnect>` tag.

The `<on_connect>` and `<on_disconnect>` scripts are optional.

IPsec VPN

IPsec VPN configurations have one options section and one or more connection details.

```
<forticlient_configuration>
<vpn>
  <ipsecvpn>
    <options>
      <show_vpn_before_logon>0</show_vpn_before_logon>
      <disconnect_on_log_off>1</disconnect_on_log_off>
      <keep_connection_alive>0</keep_connection_alive>
      <enabled>1</enabled>
      <beep_if_error>0</beep_if_error>
      <beep_continuously>0</beep_continuously>
      <beep_seconds>0</beep_seconds>
      <usewincert>1</usewincert>
      <uselocalcert>0</uselocalcert>
      <usesmcardcert>1</usesmcardcert>
```

```
    <mtu_size>1300</mtu_size>
    <use_windows_credentials>0</use_windows_credentials>
  </options>
  <connections>
    <connection>
      <name>ipsecdemo</name>
      <single_user_mode>0</single_user_mode>
      <type>manual</type>
      <ui>
        <show_passcode>0</show_passcode>
        <show_remember_password>1</show_remember_password>
        <show_alwaysup>1</show_alwaysup>
        <show_autoconnect>1</show_autoconnect>
      <tray_menu>1</tray_menu>
      <ike_settings>
        <prompt_certificate>0</prompt_certificate>
        <server>ipsecdemo.fortinet.com</server>
        <authentication_method>Preshared
            Key</authentication_method>
        <auth_key>Encdab907ed117eafaadd92f82b3e768b5414e4402dbd4
            df4585d4202c65940f1b2e9</auth_key>
        <mode>aggressive</mode>
        <dhgroup>5;</dhgroup>
        <key_life>28800</key_life>
        <localid></localid>
        <nat_traversal>1</nat_traversal>
        <mode_config>1</mode_config>
        <enable_local_lan>0</enable_local_lan>
        <nat_alive_freq>5</nat_alive_freq>
        <dpd>1</dpd>
        <dpd_retry_count>3</dpd_retry_count>
        <dpd_retry_interval>5</dpd_retry_interval>
        <enable_ike_fragmentation>0</enable_ike_fragmentation>
        <xauth>
          <enabled>1</enabled>
          <prompt_username>1</prompt_username>
          <username>Enc02355436679b004573d2a1586d399de912e37ee19
              3ba0d14</username>
          <password />
          <attempts_allowed>1</attempts_allowed>
          <use_otp>0</use_otp>
        </xauth>
        <proposals>
          <proposal>3DES|MD5</proposal>
          <proposal>3DES|SHA1</proposal>
          <proposal>AES128|MD5</proposal>
          <proposal>AES128|SHA1</proposal>
        </proposals>
      </ike_settings>
```

```
    <ipsec_settings>
      <remote_networks>
        <network>
          <addr>0.0.0.0</addr>
          <mask>0.0.0.0</mask>
        </network>
      </remote_networks>
      <dhgroup>5</dhgroup>
      <key_life_type>seconds</key_life_type>
      <key_life_seconds>1800</key_life_seconds>
      <key_life_Kbytes>5120</key_life_Kbytes>
      <replay_detection>1</replay_detection>
      <pfs>1</pfs>
      <autokey_keep_alive>0</autokey_keep_alive>
      <use_vip>1</use_vip>
      <virtualip>
        <type>modeconfig</type>
        <ip>0.0.0.0</ip>
        <mask>0.0.0.0</mask>
        <dnsserver>0.0.0.0</dnsserver>
        <winserver>0.0.0.0</winserver>
      </virtualip>
      <proposals>
        <proposal>3DES|MD5</proposal>
        <proposal>3DES|SHA1</proposal>
        <proposal>AES128|MD5</proposal>
        <proposal>AES128|SHA1</proposal>
      </proposals>
    </ipsec_settings>
    <on_connect>
      <script>
        <os>windows</os>
        <script>
        <script>
          <![CDATA[]]>
        </script>
      </script>
    </script>
  </on_connect>
  <on_disconnect>
    <script>
      <os>windows</os>
      <script>
        <script>
          <![CDATA[]]>
        </script>
      </script>
    </script>
  </on_disconnect>
```

```
      </connection>
    </connections>
    </ipsecvpn>
  </vpn>
  </forticlient_configuration>
```

The following table provides IPsec VPN XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<ipsecvpn> <options> elements		
<show_vpn_before_logon>	Display a list of configured VPN tunnels in a list on the Windows logon screen. Boolean value: [0 | 1]	0
<disconnect_on_log_off>	Drop the established VPN connection when the user logs off. Boolean value: [0 | 1]	1
<keep_connection_alive>	Retry restoring the connection of an active VPN session. Boolean value: [0 | 1]	0
<enabled>	Enable or disable IPsec VPN. Boolean value: [0 | 1]	1
<beep_if_error>	Beep if VPN connection attempt fails. Boolean value: [0 | 1]	0
<beep_continuously>	Enable or disable the continuous beep. Boolean value: [0 | 1]	1
<beep_seconds>	Enter a value for the number of seconds to beep if an error occurs.	60
<usewincert>	Use Microsoft Windows certificates for connections. Boolean value: [0 | 1]	
<uselocalcert>	Use local certificates for connections. Boolean value: [0 | 1]	
<usesmcardcert>	Use certificates on smart cards. Boolean value: [0 | 1]	
<mtu_size>	Maximum Transmit Unit (MTU) size for packets on the VPN tunnel.	
<use_windows_credentials>	Use Microsoft Windows login credentials for VPN authentication. Boolean value: [0 | 1]	

The <connections> tag may contain one or more <connection> elements. Each <connection> has the following:

- name and type: the name and type of connection
- IKE settings: information used to establish an IPsec VPN connection
- IPsec settings:
  - on_connect: a script to run right after a successful connection
  - on_disconnect: a script to run just after a disconnection

The following table provides VPN connection XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<name>	VPN connection name.	
<single_user_mode>	Enable or disable single user mode. If enabled, new and existing VPN connections cannot be established or will be disconnected if more than one user is logged in. Boolean value: [0 | 1]	0
<type>	IPSec VPN connection type. Select either: [manual | auto]	
<tray_menu>	Enable or disable the tray menu. Boolean value: [0 | 1]	1
<ui> elements		
<show_passcode>	Display *Passcode* instead of *Password* in the VPN tab in the console. Boolean value: [0 | 1]	
<show_remember_password>	Display the remember password checkbox in the console. Boolean value: [0 | 1]	
<show_alwaysup>	Display the always up checkbox in the console. Boolean value: [0 | 1]	
<show_autoconnect>	Display the autoconnect checkbox in the console. Boolean value: [0 | 1]	

The elements of the <ui> tag are set by the FortiGate following an IPsec VPN connection.

VPN connection name is mandatory. If a connection of this type and this name exists, its values will be overwritten with the new ones.

IKE settings

Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates.

The following table provides IKE setting XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
`<prompt_certificate>`	Prompt for certificate on connect. Boolean value: `[0 | 1]`	
`<server>`	IP address or FQDN.	
`<authentication_method>`	Authentication method. Select one of the following: • `Preshared Key` • `X509 Certificate` • `Smartcard X509 Certificate` • `System Store X509 Certificate`	
`<auth_key>`	An encrypted value depending on the authentication method: a preshared key or a certificate name.	
`<mode>`	Connection mode. Select either: `[aggressive | main]`	
`<dhgroup>`	A list of possible Diffie-Hellman (DH) protocol groups, separated by semi-colon.	
`<key_life>`	Phase 2 key expiry duration, in seconds.	`28800`
`<localid>`	Enter the peer ID configured in the FortiGate Phase 1 configuration. If *Accept any peer ID* has been configured, leave this field blank.	
`<nat_traversal>`	Enable or disable NAT traversal. Boolean value: `[0 | 1]`	
`<mode_config>`	Enable or disable mode configuration. Boolean value: `[0 | 1]`	
`<enable_local_lan>`	Enable or disable local LAN. Boolean value: `[0 | 1]`	

<nat_alive_freq>	NAT alive frequency.	
<dpd>	Enable or disable Dead Peer Detection (DPD). Boolean value: [0 | 1]	1
<dpd_retry_count>	Number of times to send unacknowledged DPD messages before declaring peer as dead.	3
<dpd_retry_interval>	Duration of DPD idle periods, in seconds.	5
<enable_ike_fragmentation>	Support fragmented IKE packets.	0
<xauth> elements		
<enabled>	Select to use IKE Extended Authentication (xAuth). Boolean value: [0 | 1]	
<prompt_username>	Request for a user name. Boolean value: [0 | 1]	
<username>	Either encrypted or non-encrypted user name on IPsec server.	
<password>	Either encrypted or non-encrypted password. For more information, see "Encrypted username and password" on page 8.	
<attempts_allowed>	Maximum number of failed login attempts allowed.	
<use_otp>	Use One Time Password (OTP). Boolean value: [0 | 1]	
<proposals> elements		
<proposal>	Encryption and authentication types to use, separated by a pipe. Example: <proposal>3DES|MD5<proposal> Multiple elements accepted. First setting: Encryption type: DES, 3DES, AES128, AES192, AES256 Second setting: Authentication type: MD5, SHA1, SHA256	

IPsec settings

The following table provides IPsec setting XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<remote_networks> elements		
<network>	Specifies a network address <addr> with subnet mask <mask>.	
<addr>	Network IP address.	
<mask>	Subnet mask to apply to network address <addr>.	
<dhgroup>	A list of possible Diffie-Hellman (DH) protocol groups, separated by semi-colon.	
<key_life_type>	Phase 2 key re-key duration type. Select one of the following: • seconds • kbytes • both	
<key_life_seconds>	Phase 2 key maximum life in seconds.	1800
<key_life_Kbytes>	Phase 2 key maximum life in kB.	5120
<replay_detection>	Detect an attempt to replay a previous VPN session.	
<pfs>	Enable or disable Perfect Forward Secrecy (PFS). Boolean value: [0 | 1]	
<autokey_keep_alive>	Enable or disable autokey keep alive. Boolean value: [0 | 1]	
<use_vip>	Use virtual IP. Boolean value: [0 | 1]	
<virtualip> elements		
<type>	Type of virtual IP. Select either: [modeconfig | dhcpoveripsec]	
<ip>	IP address.	
<mask>	Network mask.	
<dnsserver>	DNS server IP address.	
<winserver>	Microsoft Windows server IP address.	

<proposals> elements		
<proposal>	Encryption and authentication types to use, separated by a pipe. Example: <proposal>3DES|MD5<proposal> Multiple elements accepted. First setting: Encryption type: DES, 3DES, AES128, AES192, AES256 Second setting: Authentication type: MD5, SHA1, SHA256	

The on_connect and on_disconnect structure and scripting format are similar to that described in the section titled: SSL VPN earlier.

Certificates

Certificates are contained in the <certificates></certificates> tags. There are two subsections:

- CA certificate

  Base 64 encoded CA certificate.
- CRL

  Uses Online Certificate Status Protocol (OCSP).

```
<forticlient_configuration>
  <certicates>
  <CA_certificates/>
    <CRL>
      <OCSP>
        <enabled>1</enabled>
        <server>187.205.34.96</server>
        <port>80</port>
      </OCSP>
    </CRL>
  </certficates>
</forticlient_configuration>
```

The following table provides certificate XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<CRL> <OCSP> elements		
<enabled>	Use Online Certificate Status Protocol (OCSP). Boolean value: [0 | 1]	

<server>	Enter the server IP address.	
<port>	Enter the server port number.	

Antivirus

The Antivirus configuration data are contained in the <antivirus></antivirus> tags.

The following are subsections of the antivirus configuration.

- General options
  Options that apply to the overall operation of the antivirus service.
- Scheduled scans
  Scheduled scanning of the system.
- On-demand scans
  Details relating to on-demand scans.
- Real-time protection
  Options to use during when real-time protection scanning is activated.
- Email
  How to handle scanning of email messages.
- Quarantine
  Configures quarantine operations.
- Server
  Special options for servers.

Antivirus general options

This has options that enable or disable various services in the antivirus feature.

```
<forticlient_configuration>
  <antivirus>
    <signature_expired_notification>0</signature_expired_notificati
        on>
    <scan_on_insertion>0</scan_on_insertion>
    <shell_integration>1</shell_integration>
    <antirootkit>-1</antirootkit>
    <fortiguard_analytics>0</fortiguard_analytics>
    <multi_process_limit>0</multi_process_limit>
  </antivirus>
</forticlient_configuration>
```

The following table provides AntiVirus general option XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<signature_expired_notification>	Enable or disable expired signature notification. Boolean value: [0 | 1]	0

<scan_on_insertion>	Enable or disable scan on insertion. Boolean value: [0 | 1]	0
<shell_integration>	Enable or disable shell integration. Boolean value: [0 | 1]	1
<antirootkit>	Enable or disable anti-rootkit. Boolean value: [0 | 1]	1
<fortiguard_analytics>	Enable or disable FortiGuard Analytics. Boolean value: [0 | 1]	1
<multi_process_limit>	The number of antivirus scanning processes to use for scheduled or on-demand scans. The maximum is the number of CPU processors and cores. When set to 0, FortiClient will determine the optimal value.	0

Scheduled scans

User may schedule scanning for viruses in one of three ways:

- Full scan
  Scan the entire system.
- Quick scan
  Scan only none-system files.
- Custom scan
  Scan a selection of files, as specified by user.

Zero, one or more of these may be configured at any one time.

```
<forticlient_configuration>
  <antivirus>
    <scheduled_scans>
      <!--zero, one or more of the following child nodes-->
      <quick>
        <enabled>1</enabled>
        <repeat>1</repeat>
        <date>2012/10/30</date>
        <days>2</days>
        <day_of_month>21</day_of_month>
        <time>15:30</time>
      </quick>
      <full>
        <enabled>1</enabled>
        <repeat>1</repeat>
        <days>2</days>
        <time>18:30</time>
        <removable_media>1</removable_media>
        <network_drives>0</network_drives>
```

```
            <priority>0</priority>
          </full>
          <directory>
            <enabled>1</enabled>
            <repeat>1</repeat>
            <date>2012/10/30</date>
            <days>2</days>
            <day_of_month>21</day_of_month>
            <time>18:30</time>
            <directory>c:\users\</directory>
            <priority>2</priority>
          </directory>
        </scheduled_scans>
      </antivirus>
    </forticlient_configuration>
```

Each of three scheduling options require specification of several common elements, which define when scanning should occur. The common elements are described first. Other elements specific to the full and custom scans are described later.

The following table provides scheduled scan XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
common elements		
<enabled>	Enable or disable scheduled scan. Boolean value: [0 | 1]	
<repeat>	Frequency of scans. Select one of the following: • 0: daily • 1: weekly • 2: monthly	
<date>	Date to run scan in the format YYYY/MM/DD.	
<days>	Day of the week to run scan. Multiple days may be provided, separated by comma. Select one or more of the following: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday	

<day_of_month>	The day of the month to run a scan. A number from 1 to 31.	
<time>	Time value in 24 hour clock.	

Only one of the elements: <date>, <days>, <day_of_month> is required. The factory default at the time of installation is to run a full scan on Mondays at 18:30 hours.

The following table provides element XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<full> elements		
<removable_media>	Enable or disable scanning files on removable media. Boolean value: [0 | 1]	1
<network_drives>	Enable or disable scanning files on network drives. Boolean value: [0 | 1]	0
<priority>	Scan priority. Select one of the following: • 0: normal • 1: low • 2: high	0
<directory> elements		
<directory>	The full path to the directory to scan.	
<priority>	Scan priority. Select one of the following: • 0: normal • 1: low • 2: high	

On-Demand scans

The <on_demand_scanning> element defines how the antivirus scanner handles scanning of files manually requested by the end user.

```
<forticlient_configuration>
  <antivirus>
    <on_demand_scanning>
    <on_virus_found>0</on_virus_found>
    <pause_on_battery_power>1</pause_on_battery_power>
    <automatic_virus_submission>
      <enabled>0</enabled>
      <smtp_server>fortinetvirussubmit.com</smtp_server>
      <username />
      <password>Enc6a7457a9e3e6155dee0238dcaa8825521ae749fd66ffc32a
          </password>
    </automatic_virus_submission>
    <compressed_files>
      <scan>1</scan>
      <maxsize>0</maxsize>
    </compressed_files>
    <riskware>
      <enabled>1</enabled>
    </riskware>
    <adware>
      <enabled>1</enabled>
    </adware>
    <heuristic_scanning>1</heuristic_scanning>
    <scan_file_types>
      <all_files>1</all_files>
      <file_types>
        <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.
            ASX,.AVB,.AX,.AX2,.BAT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.
            CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.DE
            V,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.G
            VB,.HLP,.HTA,.HTM,.HTML,.HTT,.HTW,.HTX,.HXS,.INF,.INI,
            .JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB,.MHT,.MHTM,.MHT
            ML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PN
            F,.PNP,.POT,.PPA,.PPS,.PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.R
            TF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,.SHT,.SHTML,.SHW,.SIS,
            .SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS
            ,.VBX,.VOM,.VSD,.VSS,.VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WI
            Z,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.XTP</ex
            tensions>
          <include_files_with_no_extension>0</include_files_with_n
              o_extension>
      </file_types>
      </scan_file_types>
      <exclusions>
      <!--the element below can exist 0-n times-->
      <file></file>
      <!--the element below can exist 0-n times-->
```

```
            <folder></folder>
            <file_types>
               <extensions />
            </file_types>
         </exclusions>
         </on_demand_scanning>
      </antivirus>
   </forticlient_configuration>
```

The following table provides on-demand scan XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<on_virus_found>	The action FortiClient will perform if a virus is found. Select one of the following: • 0: clean • 1: ignore • 2: repair • 3: warning • 4: quarantine • 5: deny access	0
<pause_on_battery_power>	Suspend scanning when system is on battery. Boolean value: [0 | 1]	1
<heuristic_scanning>	Enable or disable heuristics signatures. Boolean value: [0 | 1]	1
<automatic_virus_submission> elements		
<enabled>	Send virus files found to FortiGuard servers. Boolean value: [0 | 1]	0
<smtp_server>	SMTP server IP address or FQDN.	fortinetvirussubmit.com
<password>	Either encrypted or non-encrypted password. For more information, see “Encrypted username and password” on page 8.	
<compressed_files> elements		
<scan>	Enable or disable scanning of compressed files. Boolean value: [0 | 1]	1
<maxsize>	Maximum compressed file size to scan in MB. A number up to 65535. 0 means no limit.	0

<riskware> elements		
<enabled>	Enable or disable scanning of riskware files. Boolean value: [0 | 1]	1
<adware> elements		
<enabled>	Enable or disable scanning of adware files. Boolean value: [0 | 1]	1
<scan_file_types> elements		
<all_files>	Enabled or disable scanning of all file types. If enabled, ignore the <file_types> element. Boolean value: [0 | 1]	1
<scan_file_types> <file_types> elements		
<extensions>	Comma separated list of extensions to scan.	
<include_files_with_no_extension>	Determines whether to scan files with no extension. Boolean value: [0 | 1]	0
<exclusions> elements		
<file>	Full path to a file to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more files.	
<folder>	Full path to a directory to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more directories.	
<exclusions> <file_types> elements		
<extensions>	Comma separated list of extensions to exclude from on-demand scanning.	

Real-time protection

The <real_time_protection> element configures how the scanner processes files used by programs running on the system.

Several tags are similar between this section and the previous one: <on_demand_scanning>.

```
<forticlient_configuration>
  <antivirus>
    <real_time_protection>
      <enabled>1</enabled>
      <when>0</when>
      <on_virus_found>0</on_virus_found>
      <popup_alerts>0</popup_alerts>
      <popup_registry_alerts>0</popup_registry_alerts>
      <compressed_files>
        <scan>1</scan>
        <maxsize>2</maxsize>
      </compressed_files>
      <riskware>
        <enabled>1</enabled>
      </riskware>
      <adware>
        <enabled>1</enabled>
      </adware>
      <heuristic_scanning>
        <enabled>0</enabled>
        <action>0</action>
      </heuristic_scanning>
      <scan_file_types>
        <all_files>1</all_files>
        <file_types>
        <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.
             ASX,.AVB,.AX,.AX2,.BAT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.
             CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.DE
             V,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.G
             VB,.HLP,.HTA,.HTM,.HTML,.HTT,.HTW,.HTX,.HXS,.INF,.INI,
             .JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB,.MHT,.MHTM,.MHT
             ML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PN
             F,.PNP,.POT,.PPA,.PPS,.PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.R
             TF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,.SHT,.SHTML,.SHW,.SIS,
             .SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS
             ,.VBX,.VOM,.VSD,.VSS,.VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WI
             Z,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.XTP</ex
             tensions>
        <include_files_with_no_extension>0</include_files_with_no_
             extension>
        </file_types>
      </scan_file_types>
      <exclusions>
        <!--the element below can exist 0-n times-->
        <!--the element below can exist 0-n times-->
```

```
        <file_types>
          <extensions />
        </file_types>
      </exclusions>
    </real_time_protection>
    </antivirus>
</forticlient_configuration>
```

The following table provides real time protection XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<enabled>	Enable or disable real time protection. Boolean value: [0 | 1]	1
<when>	File I/O activities that result in a scan. Select one of the following: • 0: read and write • 1: only on read • 2: only on write	0
<on_virus_found>	The action FortiClient will perform if a virus is found. Select one of the following: • 0: clean • 1: ignore • 2: repair • 3: warning • 4: quarantine • 5: deny access	5
<popup_alerts>	Display alerts when a virus is found. Boolean value: [0 | 1]	1
<popup_registry_alerts>	Enable or disable pop-up registry alerts. This feature displays alerts if a process tries to change registry start items. Boolean value: [0 | 1]	0
<compressed_files> elements		
<scan>	Enable or disable scanning of compressed files. Boolean value: [0 | 1]	1
<maxsize>	Maximum compressed file size to scan in MB. A number up to 65535. 0 means no limit.	2

<riskware> elements		
<enabled>	Enable or disable scanning of riskware files. Boolean value: [0 | 1]	1
<adware> elements		
<enabled>	Enable or disable scanning of adware files. Boolean value: [0 | 1]	1
<heuristic_scanning> elements		
<enabled>	Enable or disable heuristics signatures. Boolean value: [0 | 1]	0
<action>	The action FortiClient will perform if a virus is found. Select either: • 0: warning • 1: deny access	
<scan_file_types> elements		
<all_files>	Enabled or disable scanning of all file types. If enabled, ignore the <file_types> element. Boolean value: [0 | 1]	1
<scan_file_types> <file_types> elements		
<extensions>	Comma separated list of extensions to scan.	
<include_files_with_no_extension>	Determines whether to scan files with no extension. Boolean value: [0 | 1]	0
<exclusions> elements		
<file>	Full path to a file to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more files.	
<folder>	Full path to a directory to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more directories.	
<exclusions> <file_types> elements		
<extensions>	Comma separated list of extensions to exclude from on-demand scanning.	

Email

Emails will be scanned for viruses based on the settings in the <email> tag. You can configure virus scanning for SMTP, POP3, and Microsoft Outlook.

```
<forticlient_configuration>
  <antivirus>
    <email>
      <smtp>1</smtp>
      <pop3>1</pop3>
      <outlook>1</outlook>
      <wormdetection>
        <enabled>0</enabled>
        <action>0</action>
      </wormdetection>
      <heuristic_scanning>
        <enabled>0</enabled>
        <action>0</action>
      </heuristic_scanning>
    </email>
  </antivirus>
</forticlient_configuration>
```

The following table provides email XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<smtp>	When enabled, scan email messages sent through SMTP protocol. Boolean value: [0 | 1]	1
<pop3>	Determines whether to scan email messages received through POP3 protocol. Boolean value: [0 | 1]	1
<outlook>	Scan email files processed through Microsoft Outlook. Boolean value: [0 | 1]	1
<wormdetection> elements		
<enabled>	Scan for worm viruses. Boolean value: [0 | 1]	0
<action>	The action FortiClient will perform if a virus is found. Select either: • 0: warn • 1: terminate process	0
<heuristic_scanning> elements		

<enabled>	Enable or disable heuristics signatures. Boolean value: [0 | 1]	0
<action>	The action FortiClient will perform if a virus is found. Select either: • 0: log and warn • 1: strip and quarantine	0

Quarantine

The maximum age for quarantined files is specified in the <quarantine> tag.

```
<forticlient_configuration>
  <antivirus>
    <quarantine>
      <cullage>100</cullage>
    </quarantine>
  </antivirus>
</forticlient_configuration>
```

The following table provides quarantine XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<cullage>	How long to hold quarantined files, in days, before deleting them. A number from 1 to 365.	100

Server

On Microsoft Windows servers, it may be desired to exclude system files from being scanned. These are configured in the <server> tag.

```
<forticlient_configuration>
  <antivirus>
    <server>
      <exchange>
        <integrate>0</integrate>
        <action>0</action>
        <excludefilesystemfromscanning>0</excludefilesystemfromsca
            nning>
        <excludefileextensionsfromscanning>0</excludefileextension
            sfromscanning>
    </exchange>
    <sqlserver>
        <excludefilesystemfromscanning>0</excludefilesystemfromsca
            nning>
        <excludefileextensionsfromscanning>0</excludefileextension
            sfromscanning>
```

```
        </sqlserver>
      </server>
    </antivirus>
  </forticlient_configuration>
```

The following table provides server XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<exchange> elements		
<integrate>	Boolean value: [0 | 1]	0
<action>	The action FortiClient will perform if a virus is found. Select either: • 0: Quarantine • 1: Remove Attachment Only	0
<excludefilesystemfromscanning>	Enable to exclude file system from scanning. Boolean value: [0 | 1]	0
<excludefileextensionsfromscanning>	Enable to exclude file extensions from scanning. Boolean value: [0 | 1]	0
<sqlserver> elements		
<excludefilesystemfromscanning>	Enable to exclude file system from scanning. Boolean value: [0 | 1]	0
<excludefileextensionsfromscanning>	Enable to exclude file extensions from scanning. Boolean value: [0 | 1]	0

Endpoint Control

Endpoint Control configuration elements are usually downloaded from a FortiGate following registration of a FortiClient user to the same FortiGate. There are two sections:

- Endpoint Control general attributes.

  These are contained in the `<endpoint_control></endpoint_control>` tags.
- Configuration details relating to specific FortiClient services, such as Antivirus, Web Filtering, Application Firewall, Vulnerability Scanner, and so on. These will be found in the respective configuration elements of the services affected.

Endpoint control general attributes are listed below.

```
<forticlient_configuration>
  <endpoint_control>
    <checksum></checksum>
    <enabled>1</enabled>
    <!--short keepalive timeout in ms-->
    <keepalive_short_timeout>20000</keepalive_short_timeout>
    <!--keepalive timeout in seconds-->
    <keepalive_timeout>1800</keepalive_timeout>
    <custom_ping_server />
    <ping_server>172.17.61.178:8010</ping_server>
    <fgt_name>al-fwf81cm</fgt_name>
    <fgt_sn>Encfbbd55bd8205d2be3d0e9dece908e28cb732118b3f9a66db1f61
        643fd9dbc392a3c9616fac489a42aaaffa109f46f38eeadcf5be049aea
        c552e87713662ffdea58a25e67beec16c12fb8f3b1eafd4c8e9692c85c
        3cfa9066bb</fgt_sn>
    <offnet_update>1</offnet_update>
    <corporate_id>Enc7fde88aa0ec0b48dc8841525808604007a76fc7f01e8c5
        ce3cd77c8c2c372375e0e45acd6b<corporate_id>
    <user>Encaa0ec0b48d07a76fc7c88415258086040f01e8c5ce3c5e0e45a7fd
        e88d77c8c2c37237cd6b</user>
    <skip_confirmation>0</skip_confirmation>
    <disable_unregister>0</disable_unregister>
    <fgt_logoff_on_fct_shutdown>1</fgt_logoff_on_fct_shutdown>
    <show_bubble_notifications>0</show_bubble_notifications>
    <conf_recv_time></conf_recv_time>
    <vdom>root</vdom>
    <disable_unregister>0</disable_unregister>
    <silent_registration>0</silent_registration>
    <show_bubble_notifications>1</show_bubble_notifications>
    <fgt_list>Enc256828d1e23febfa0b789324ea1fc9cf45acdc8af3888e7aa2
        6677825bbf8d5d123fcbc2884f3cb3f2a03b5414ab01e6a6c22762add0
        c4f209224f052dec29491e1d15eee4a1a290a81b367c3d4a5251258ed1
        4921e231547f52d9e3</fgt_list>
    <ui>
      <display_antivirus>1</display_antivirus>
      <display_webfilter>1</display_webfilter>
      <display_firewall>1</display_firewall>
      <display_vpn>1</display_vpn>
      <display_vulnerability_scan>1</display_vulnerability_scan>
```

```
        <registration_dialog>
          <show_profile_details>1</show_profile_details>
        </registration_dialog>
      </ui>
      <fortigates>
        <fortigate>
          <serial_number/>
          <name/>
          <registration_password/>
          <address/>
        </fortigate>
      </fortigates>
    </endpoint_control>
  </forticlient_configuration>
```

The following table provides endpoint control XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<checksum>	Configuration checksum calculated on and enforced by the FortiGate.	
<enabled>	Enable endpoint control.	
<keepalive_short_timeout>	Short keepalive timeout in ms.	20000
<keepalive_timeout>	Keepalive timeout in seconds.	1800
<custom_ping_server>	IP address or FQDN.	
<ping_server>	IP address or FQDN.	
<fgt_name>	Name of the FortiGate currently registered to (if any).	
<fgt_sn>	Encrypted serial number of the registered FortiGate (if any).	
<offnet_update>	Enable synchronization of configuration updates from the FortiGate. Boolean value: [0 | 1]	1
<corporate_id>	Encrypted password required to connect to the FortiGate.	
<user>	Encrypted user name.	
<skip_confirmation>	Do not prompt user before proceeding to complete registration with a FortiGate. Boolean value: [0 | 1]	0

<disable_unregister>	Prevent standard user from being able to unregister after successfully registering to a FortiGate device. Boolean value: [0 | 1]	0
<fgt_logoff_on_fct_shutdown>	Notify FortiGate when FortiClient is shut down. Boolean value: [0 | 1]	1
<show_bubble_notifications>	Notify the user when new policies are installed. Boolean value: [0 | 1]	1
<conf_recv_time>	Time of the most recently received configuration.	
<vdom>	Name of the FortiGate VDOM that the client is registered to.	
<disable_unregister>	User cannot unregister once registered. Boolean value: [0 | 1]	0
<silent_registration>	Register to the FortiGate without prompting the user. Boolean value: [0 | 1]	0
<show_bubble_notification>	Show notifications in the system tray when a configuration update is received from the FortiGate. Boolean value: [0 | 1]	1
<fgt_list>	Encrypted list of remembered FortiGates.	
<ui> elements		
<display_antivirus>	Display the Antivirus tab in the console. Boolean value: [0 | 1]	
<display_webfilter>	Display the Web Filtering tab in the console. Boolean value: [0 | 1]	
<display_vpn>	Display the Remote Access (VPN) tab in the console. Boolean value: [0 | 1]	
<display_vulnerability_scan>	Display the Vulnerability Scan tab in the console. Boolean value: [0 | 1]	
<registration_dialog> element		

<show_profile_details>	Present to user before registration the details of the endpoint profile that will be installed once registration is completed. Boolean value: [0 | 1]	
<fortigates> <fortigate> elements		
<serial_number>	The serial number of the FortiGate.	
<name>	The name of the FortiGate.	
<regsitration_password>	Registration password for this FortiGate, if required.	
<addresses>	IP address or FQDN. Multiple IP addresses may be entered, separated by semicolons.	

Log elements are non-functional in FortiClient v5.0.0, and v5.0 Patch Release 1. In FortiClient v5.0 Patch Release 2, these elements will be moved to the logging section of the XML configuration, and will be used to control upload frequency.

The <fortigate> element is used to define the FortiGates in a roaming (or redundant) FortiGate configuration. One or more <fortigate> elements may be provided within <fortigates>.

The following elements are set by the FortiGate. FortiClient reads them and imports into its configuration when received from the FortiGate. If modified by the user locally on the Windows system, FortiClient will ignore the changes.

```
<vdom>
<disable_unregister>
<ui>
```

For the other elements that could be modified locally, If the same element is received from the FortiGate, the existing value will be overwritten.

The following elements affect Endpoint Control.

Enable or disable display of advertisements.

```
<forticlient_configuration>
  <system>
    <ui>
      <ads>1</ads>
    </ui>
  </system>
</forticlient_configuration>
```

Enable antivirus real-time protection.

```
<forticlient_configuration>
  <antivirus>
    <real_time_protection>
      <enabled>1</enabled>
    <real_time_protection>
  </antivirus>
```

```
</forticlient_configuration>
```

Other services that may be configured from the FortiGate will usually use the full set of configuration elements available to them, as described in the various sections of this documents. These include the following:

```
<forticlient_configuration>
  <system>
    <update>
    </update>
    <log_settings>
    </log_settings>
  </system>
  <vpn>
  </vpn>
  <firewall>
  </firewall>
  <webfilter>
  </webfilter>
  <vulnerability_scan>
  </vulnerability_scan>
</forticlient_configuration>
```

Single Sign-On Mobility Agent

Configuration elements for FortiClient Single Sign-On Mobility Agent are contained in the `<fssoma></fssoma>` tags.

```
<forticlient_configuration>
  <fssoma>
    <enabled>0</enabled>
    <serveraddress />
    <presharedkey>Enc5ec0701e014e7e36a1c6a53aeba87af13c5e9e49c6621098</presharedkey>
  </fssoma>
</forticlient_configuration>
```

The following table provides Single Sign-On XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
`<enabled>`	Enable or disable Single Sign On (SSO). Boolean value: `[0 | 1]`	`0`
`<serveraddress>`	FortiAuthenticator IP address or FQDN.	
`<presharedkey>`	Encrypted or unencrypted pre-shared key.	

To enable the FortiClient SSO Mobility agent service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the *FortiAuthenticator v2.2 Administration Guide* at http://docs.fortinet.com. For information on purchasing a FortiClient license, please contact your authorized Fortinet reseller.

WAN Optimization

WAN Optimization is configured in the `<wan_optimization></wan_optimization>` tags.

```
<forticlient_configuration>
  <wan_optimization>
    <enabled>0</enabled>
    <support_http>1</support_http>
    <support_cifs>1</support_cifs>
    <support_mapi>1</support_mapi>
    <support_ftp>1</support_ftp>
    <max_disk_cache_size_mb>512</max_disk_cache_size_mb>
  </wan_optimization>
</forticlient_configuration>
```

The following table provides WAN Optimization XML tags, the description, and the default value (if applicable).

XML Tag	Description	Default Value
`<enabled>`	Enable or disable WAN Optimization. Boolean value: `[0 | 1]`	`0`
`<support_http>`	Enable or disable HTTP support. Boolean value: `[0 | 1]`	`1`
`<support_cifs>`	Enable or disable CIFS support. Boolean value: `[0 | 1]`	`1`
`<support_mapi>`	Enable or disable MAPI support. Boolean value: `[0 | 1]`	`1`
`<support_ftp>`	Enable or disable FTP support. Boolean value: `[0 | 1]`	`1`
`<max_disk_cache_size_mb>`	Maximum disk cache size in MB.	`512`

Web Filtering

Web Filtering XML configurations are contained in the <webfilter></webfilter> tags.

There are two main sections:

- General options

  Configuration elements that affect the whole of the web filtering service.
- Profiles

  Defines one or more rules that will be applied to network traffic.

```
<forticlient_configuration>
  <webfilter>
    <https_enabled>1</https_enabled>
    <!--use enable_filter to enable/disable WebFiltering-->
    <enable_filter>1</enable_filter>
    <!--enabled enables/disables the FortiGuard querying service.-->
    <enabled>1</enabled>
    <log_all_urls>0</log_all_urls>
    <block_uncategorised>0</block_uncategorised>
    <white_list_has_priority>0</white_list_has_priority>
    <current_profile>0</current_profile>
    <partial_match_host>0</partial_match_host>
    <disable_when_managed>0</disable_when_managed>
    <max_violations>250</max_violations>
    <max_violations_age>7</max_violations_age>
    <fortiguard>
      <url>fgd1.fortigate.com</url>
      <enabled>1</enabled>
      <block_unrated>0</block_unrated>
      <rate_ip_addresses>1</rate_ip_addresses>
    </fortiguard>
    <profiles>
      <profile>
        <id>0</id>
        <cate_ver>6</cate_ver>
        <description>deny</descxription>
        <name>deny</name>
        <temp_whitelist_timeout>300</temp_whitelist_timeout>
        <categories>
          <category>
            <id>3
              <!--Hacking (Potentially Liable)-->
            </id>
            <action>deny</action>
          </category>
          <category>
            <id>4
              <!--Illegal or Unethical (Potentially Liable)-->
            </id>
```

```
            <action>deny</action>
          </category>
          <category>
            <id>5
              <!--Discrimination (Potentially Liable)-->
            </id>
            <action>deny</action>
          </category>
        </categories>
        <urls>
          <url>
            <address>www.playbpy.com</address>
            <action>deny</action>
          </url>
            <address>www.fortinet.com</address>
            <action>allow</action>
          </url>
        </urls>
    </profile>
    <profile>
      <id>2</id>
      <cate_ver>6</cate_ver>
      <description>deny</description>
      <name>deny</name>
      <temp_whitelist_timeout>300</temp_whitelist_timeout>
      <categories>
        <category>
          <id>26
            <!--Malicious Websites (Security Risk)-->
          </id>
          <action>deny</action>
        </category>
        <category>
          <id>86
            <!--Spam URLs (Security Risk)-->
          </id>
          <action>deny</action>
        </category>
      </categories>
      <safe_search>
        <enabled>1</enabled>
        <search_engines>
          <enabled>1</enabled>
          <engine>
            <name>bing</name>
            <host>
              <![CDATA[www\.bing\.com]]></host>
            <url>
```

```
            <![CDATA[^(\/images|\/videos)\/search]]></url>
          <query>
            <![CDATA[q=]]></query>
          <safe_search_string>
            <![CDATA[adlt=strict]]></safe_search_string>
          <cookie_name><![CDATA[]]</cookie_name>
          <cookie_value><![CDATA[]]</cookie_value>
        </engine>
        <engine>
          <name>google</name>
          <host>
            <![CDATA[.*\.google\..*]]></host>
          <url>
            <![CDATA[^\/((custom|search|images|videosearch|webh
                p)\?)]]></url>
          <query>
            <![CDATA[q=]]></query>
          <safe_search_string>
            <![CDATA[&safe=active]]></safe_search_string>
        </engine>
        <engine>
          <name>yahoo</name>
          <host>
            <![CDATA[.*\.yahoo\..*]]></host>
          <url>
            <![CDATA[^\/search(\/video|\/images){0,1}(\?|;)]]><
                /url>
          <query>
            <![CDATA[p=]]></query>
          <safe_search_string>
            <![CDATA[&vm=r]]></safe_search_string>
        </engine>
        <engine>
          <name>yandex</name>
          <host>
            <![CDATA[yandex\..*]]></host>
          <url>
            <![CDATA[^\/yandsearch?\?]]></url>
          <query>
            <![CDATA[text=]]></query>
          <safe_search_string>
            <![CDATA[yandex=1]]></safe_search_string>
        </engine>
      </search_engines>
      <youtube_education_filter>
        <enabled>1</enabled>
          <filter_id>
            <![CDATA[TkZEbkhj6lafXjw2-aQZcw]]></filter_id>
        </youtube_education_filter>
```

```
            </safe_search>
          </profile>
        </profiles>
      </webfilter>
    </forticlient_configuration>
```

The general options are described first.

The following table provides Web Filtering XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<https_enabled>	Enable or disable Web Filtering on HTTPS traffic. Boolean value: [0 | 1]	1
<enable_filter>	Enable or disable Web Filtering. Boolean value: [0 | 1]	1
<enabled>	Enable or disable FortiGuard querying service. Boolean value: [0 | 1]	1
<log_all_urls>	Record all visited URLs to the log file, both blocked and allowed. Boolean value: [0 | 1]	0
<block_uncategorised>	Block network traffic that does not match any rules. Boolean value: [0 | 1]	0
<white_list_has_priority>	If traffic matches both a block and an allow rule, it should be allowed. Boolean value: [0 | 1]	0
<current_profile>	Currently selected profile ID. (optional)	
<partial_match_host>	A hostname that is a substring of the specified path is treated as a full match. Boolean value: [0 | 1]	0
<disable_when_managed>	If set to 1 (true), Web Filtering will be disabled when FortiClient is registered to a FortiGate using Endpoint Control. Boolean: [0 | 1]	
<max_violations>	Maximum number of violations stored at any one. A number from 250 to 5000.	5000

<max_violation_age>	Maximum age in days of a violation record before it is culled. A number from 1 to 90.	90
<fortiguard> elements		
<url>	IP address or FQDN of the FortiGuard server.	fgd1.fortigate.com
<enabled>	Enable or disable use of FortiGuard servers. Boolean value: [0 | 1]	1
<block_unrated>	Block unrated URLs. Boolean value: [0 | 1]	0
<rate_ip_addresses>	Rate IP addresses. Boolean value: [0 | 1]	1
<profiles> <profile> <safe_search> elements		
<enabled>	Enable safe search. Boolean value: [0 | 1]	
<profiles> <profile> <safe_search> <search_engines> <engine> elements		
<enabled>	Enable safe search for the predefined search engines. Boolean value: [0 | 1]	

The <profiles> element may have one or more profiles, defined in the <profile> tag. Each <profile>, in turn, has one or more <category>, <url> and <safe_search> tags, along with other elements.

The following table provides profile XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<profile> elements		
<id>	Unique ID. A number to define the profile.	
<cate_ver>	FortiGuard category version used in this profile. A number.	6
<description>	Summary describing this profile.	
<name>	A descriptive name for the profile.	
<temp_whitelist_timeout>	The duration, in seconds, of a bypass that is applied to a page that generated a *warning*, but for which the user selected *continue*.	300

<profile> <categories> <category> elements		
<id>	Unique ID. A number. The valid set of category IDs is predefined, and is listed in exported configuration files.	
<action>	Action to perform on matching network traffic. Select one of the following: • deny • warn • monitor	
<profile> <urls> <url> elements		
<address>	URL	
<action>	Action to perform on matching network traffic. Select either: [allow | deny]	

The <safe_search> element has two main components:

- Search engines <search_engines>

  Users may define safe search parameters for each of the popular search engines: Google, Bing, Yahoo! and Yandex. Subsequent use of the engines for web searches will have safe search enabled.
- YouTube education filter <youtube_education_filter>

Educational institutions with valid YouTube education ID can provide this in the <youtube_education_filter> element to restrict YouTube contents appropriately.

The following table provides profile XML tags and the description. See the <safe_search> listing in the previous pages for examples of each tag.

XML Tag	Description	Default Value
<profiles> <profile> <safe_search> <search_engines> <engine> elements		
<name>	Name of the safe search profile.	
<host>	The FQDN of the search engine. FortiClient will monitor attempts to visit this address.	
<url>	The URL substring to match or monitor, along with the FQDN.	
<query>	The query string that will be appended to the URL.	
<safe_search_string>	The correct safe search string that will be appended to the URL for the specified engine.	

<cookie_name>	The name of the cookie to send the search engine.	
<cookie_value>	The cookie value to send the search engine.	
<profiles> <profile> <safe_search> <youtube_education_filter> elements		
<enabled>	Enable YouTube education filter. Boolean value: [0 | 1]	
<filter_id>	The institutions education identifier.	

Other than the <name> and <enabled> elements, the values for each of the elements in the previous table should be wrapped in <![CDATA[]]> XML tags. Here is an example for a <host> element taken from the <safe_search> listing.

```
<host><![CDATA[yandex\..*]]></host>
```

See http://support.google.com/youtube/bin/answer.py?hl=en&answer=2592715 for more information on YouTube for schools and the education filter.

Application Firewall

Application Firewall configuration data is contained in <firewall></firewall> tags.

The set of elements may be grouped into two:

- General options

  Options that apply to the entire firewall activities.
- Profiles

  Defines the applications and the actions to apply to them.

```
<forticlient_configuration>
  <firewall>
    <enabled>1</enabled>
    <current_profile>0</current_profile>
    <default_action>Pass</default_action>
    <show_bubble_notifications>0</show_bubble_notifications>
    <max_violations>250</max_violations>
    <max_violations_age>7</max_violations_age>
    <profiles>
      <profile>
        <id>0</id>
        <rules>
          <rule>
            <action>Block</action>
            <enabled>1</enabled>
            <application>
              <id>16783</id>
            </application>
        </rule>
          <rule>
            <action>Block</action>
```

```
                <enabled>1</enabled>
                <category>
                <id>2</id>
                </category>
              </rule>
            </rules>
          </profile>
          <!--
This is a table of all Application Firewall categories (Id ==>
     Category Name)
-->
     </profiles>
   </firewall>
</forticlient_configuration>
```

The following table provides Application Firewall XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<enabled>	Enable or disable Application Firewall. Boolean value: [0 | 1]	1
<current_profile>	Currently selected profile ID.	
<default_action>	Action to enforce on traffic that does not match any of the profiles defined. Select one of the following: • block • reset • pass	pass
<show_bubble_notifications>	Display a bubble message each time an application is blocked for matching a profile. Boolean value: [0 | 1]	
<max_violations>	Maximum number of violations stored at any one. A number from 250 to 5000	5000
<max_violation_age>	Maximum age in days of a violation record before it is culled. A number from 1 to 90.	90

The <profiles> tag may contain one or more <profile> tags, each of which has a <rules> element. The <rules> element may, itself, have zero or more <rule> tags.

The following filter elements may be used to define applications in a <rule> tag:

```
<category>
<vendor>
<behavior>
<technology>
```

<protocol>
<application>
<popularity>

If the <application> element is present, all other sibling elements (listed above) will be ignored. If it is not, a given application must match all of the provided filters to trigger the rule.

Each of these seven elements is a container for the tag: <ids>, which is a list of the identifiers (numbers) selected for that particular filter. The full <firewall> profile listed at the beginning of this section shows several examples of the use of filters within the <rule> element. Using an <ids> value all will select all matching applications.

The following table provides profile element XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
<profile> elements		
<id>	Unique ID. A unique ID number.	
<profile> <rules> <rule> elements		
<action>	Action to enforce on traffic that matches this rule. Select one of the following: • block • reset • pass	
<enabled>	Enable or disable this rule. Boolean value: [0 | 1]	1
<category>	Categories of the applications to apply <action> on.	csv list
<vendor>	Vendors of the applications to apply <action> on.	csv list
<behavior>	Behavior of the applications to apply <action> on.	csv list
<technology>	Technologies used by the applications to apply <action> on.	csv list
<protocol>	Protocols used by the applications to apply <action> on.	csv list
<application>	Identifiers (IDs) of the applications to apply <action> on.	csv list
<popularity>	Popularity of the applications to apply <action> on.	csv list

Vulnerability Scan

Configurations for Vulnerability Scan are contained in the `<vulnerability_scan></vulnerability_scan>` tags.

```
<forticlient_configuration>
  <vulnerability_scan>
    <enabled>1</enabled>
    <scan_on_fgt_registration>0</scan_on_fgt_registration>
    <scheduled_scans>
      <!-- currently there can only be one scheduled item -->
      <schedule>
        <enable_schedule>0</enable_schedule>
        <repeat>0</repeat>
        <type>24</type>
        <day>3</day>
        <time>19:30</time>
      <schedule>
    </scheduled_scans>
  </vulnerability_scan>
</forticlient_configuration>
```

The following table provides Vulnerability Scan XML tags, the description, and the default value (where applicable).

XML Tag	Description	Default Value
`<enabled>`	Vulnerability Scan is enabled.	
`<scan_on_fgt_registration>`	Scan system on FortiGate registration. Boolean value: `[0 | 1]`	`0`
`<scheduled_scans> <schedule> elements`		
`<enable_schedule>`	Enable or disable schedule. Boolean value: `[0 | 1]`	
`<repeat>`	Frequency of scans. Select one of the following: • `0: daily` • `1: weekly` • `2: monthly`	
`<type>`	Type of vulnerability scan. Select one of the following: • `8: high` • `16: critical` • `24: high & critical`	`24`

<day>	If the <repeat> tag is set to 0 (daily), the <day> tag is ignored. If the <repeat> tag is set to 1 (weekly), <day> is the day of the week to run scan. Select one of the following: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday If the <repeat> tag is set to 2 (monthly), <day> is the day of the month to run a scan. A number from 1 to 31.	The default is the date the policy was installed from the FortiGate.
<time>	Time value in 24 hour clock.	The default is the time the policy was installed from the FortiGate.

Example XML Configurations

FortiClient XML configuration

The FortiClient configuration file is user editable. The file uses XML format for easy parsing and validation. The configuration file is inclusive of all client configurations, and references the client certificates.

Design considerations

Input validation

The import function performs basic validation, and writes to log when errors or warnings are found. Default values for omitted items are defined for VPN connections. For other settings omitted values are ignored.

Handling of password fields

When exporting, the password and username fields will be encrypted (prefixed with “Enc”). However, the import function is able to take either the clear text or encrypted format.

Segment of configuration file

It is valid to import the segment of a configuration file. However, the segment should follow the syntax and level defined in this document. For example, this is a valid segment:

```
<?xml version=”1.0” encoding=”utf-8”?>
<forticlient_configuration>
  <VPN>
    <SSLVPN>
      <connections>
        <connection>
          // connection 1
        </connection>
      </connections>
    </SSLVPN>
  </VPN>
</forticlient_configuration>
```

This is not a valid segment:

```
<?xml version=”1.0” encoding=”utf-8”?>
  <connections>
    <connection>
      // connection 1
    </connection>
  </connections>
```

Client certificate

The configuration file will include the client certificate(s) when exported in an encrypted format.

Example FortiClient XML configuration file (Microsoft Windows)

The following is an example FortiClient XML configuration file. VPN autoconnect and always up are enabled in the configuration.

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
    <forticlient_version>5.0.5.308</forticlient_version>
    <version>5.0</version>
    <date>2013/08/08</date>
    <partial_configuration>0</partial_configuration>
    <os_version>windows</os_version>
    <system>
        <ui>
            <ads>1</ads>
            <default_tab>AV</default_tab>
            <flashing_system_tray_icon>1</flashing_system_tray_icon>
            <hide_system_tray_icon>0</hide_system_tray_icon>
            <suppress_admin_prompt>0</suppress_admin_prompt>
            <password />
            <culture_code>en-us</culture_code>
            <gpu_rendering>0</gpu_rendering>
        </ui>
        <log_settings>
            <level>6</level>
           <!--0=emergency, 1=alert, 2=critical, 3=error, 4=warning, 5=notice,
6=info, 7=debug, -->

<log_events>ipsecvpn,sslvpn,scheduler,update,firewall,av,proxy,shield,webfilte
r,endpoint,fssoma,wanacc,configd,vuln</log_events>
            <!--ipsecvpn=ipsec vpn, sslvpn=ssl vpn, firewall=firewall,
av=antivirus, webfilter=webfilter, vuln=vulnerability scan, wanacc=wan
acceleration, fssoma=single sign-on mobility for fortiauthenticator,
scheduler=scheduler, update=update, proxy=fortiproxy, shield=fortishield,
endpoint=endpoint control, configd=configuration, -->
            <remote_logging>
                <log_upload_enabled>0</log_upload_enabled>
                <log_upload_server />
                <log_upload_ssl_enabled>1</log_upload_ssl_enabled>
                <log_retention_days>90</log_retention_days>
                <log_upload_freq_hours>90</log_upload_freq_hours>
                <netlog_categories>7</netlog_categories>
            </remote_logging>
        </log_settings>
        <proxy>
```

```
            <update>0</update>
            <online_scep>0</online_scep>
            <virus_submission>0</virus_submission>
            <type>http</type>
            <address />
            <port>80</port>
            <username>Enc
fc2ac8eb685e35c1e734034c027cb6e411976aae15954974</username>
            <password>Enc
1eaaaf373ee51b441ec219d1f0979af45e8f2d35428c8bc5</password>
        </proxy>
        <update>
            <use_custom_server>0</use_custom_server>
            <server />
            <port>80</port>
            <timeout>60</timeout>
            <failoverport>8000</failoverport>
            <fail_over_to_fdn>1</fail_over_to_fdn>
            <update_action>notify_only</update_action>
            <scheduled_update>
                <enabled>1</enabled>
                <type>interval</type>
                <daily_at>03:00</daily_at>
                <update_interval_in_hours>3</update_interval_in_hours>
            </scheduled_update>
        </update>
        <fortiproxy>
            <enabled>1</enabled>
            <enable_https_proxy>1</enable_https_proxy>
            <http_timeout>60</http_timeout>
            <client_comforting>
                <pop3_client>1</pop3_client>
                <pop3_server>1</pop3_server>
                <smtp>1</smtp>
            </client_comforting>
            <selftest>
                <enabled>1</enabled>
                <last_port>65535</last_port>
                <notify>1</notify>
            </selftest>
        </fortiproxy>
    </system>
    <vpn>
        <options>
            <current_connection_name>SSL</current_connection_name>
            <current_connection_type>ssl</current_connection_type>
```

```
            <autoconnect_tunnel />
            <keep_running_max_tries>0</keep_running_max_tries>
            <save_password>0</save_password>
            <minimize_window_on_connect>1</minimize_window_on_connect>
            <allow_personal_vpns>1</allow_personal_vpns>
            <show_vpn_before_logon>0</show_vpn_before_logon>
            <use_windows_credentials>1</use_windows_credentials>
            <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
            <show_negotiation_wnd>0</show_negotiation_wnd>
        </options>
        <sslvpn>
            <options>
                <enabled>1</enabled>
            </options>
            <connections>
                <connection>
                    <name>SSL</name>
                    <server>ssl.fortinet.com:443</server>
                    <username>Enc
81bf1751cfd79d20f939691e1ba109c6c25f6aedbc166f13dd99315ac57bcdb589e8</username
>
                    <single_user_mode>0</single_user_mode>
                    <ui>
                        <show_remember_password>0</show_remember_password>
                    </ui>
                    <password />
                    <certificate />

<warn_invalid_server_certificate>0</warn_invalid_server_certificate>
                    <prompt_certificate>0</prompt_certificate>
                    <prompt_username>1</prompt_username>
                    <on_connect>
                        <script>
                            <os>windows</os>
                            <script>
                                <!--Write MS DOS batch script inside the CDATA
tag below.
One line per command, just like a regular batch script file.
The script will be executed in the context of the user that connected the
tunnel.
Wherever you write #username# in your script, it will be automatically
substituted with the xauth username of the user that connected the tunnel.
Wherever you write #password# in your script, it will be automatically
substituted with the xauth password of the user that connected the tunnel.
Remember to check your xml file before deploying to ensure that carriage
returns/line feeds are present.
-->
                                <script>
```

```
                                    <![CDATA[
mkdir %temp%\jose
]]></script>
                            </script>
                        </script>
                    </on_connect>
                    <on_disconnect>
                        <script>
                            <os>windows</os>
                            <script>
                                <!--Write MS DOS batch script inside the CDATA
tag below.
One line per command, just like a regular batch script file.
The script will be executed in the context of the user that connected the
tunnel.
Wherever you write #username# in your script, it will be automatically
substituted with the xauth username of the user that connected the tunnel.
Wherever you write #password# in your script, it will be automatically
substituted with the xauth password of the user that connected the tunnel.
Remember to check your xml file before deploying to ensure that carriage
returns/line feeds are present.
-->
                                <script>
                                    <![CDATA[
rmdir %temp%\jose
]]></script>
                            </script>
                        </script>
                    </on_disconnect>
                </connection>
            </connections>
        </sslvpn>
        <ipsecvpn>
            <options>
                <enabled>1</enabled>
                <beep_if_error>0</beep_if_error>
                <usewincert>1</usewincert>
                <uselocalcert>0</uselocalcert>
                <usesmcardcert>1</usesmcardcert>
            </options>
            <connections>
                <connection>
                    <name>IPSec</name>
                    <single_user_mode>0</single_user_mode>
                    <!--when single_user_mode=1 the tunnel cannot be connected
if more than one user is logged on the computer-->
                    <type>manual</type>
```

```
                        <ui>
                            <show_passcode>0</show_passcode>
                            <show_remember_password>0</show_remember_password>
                            <show_alwaysup>0</show_alwaysup>
                            <show_autoconnect>0</show_autoconnect>
                        </ui>
                        <ike_settings>
                            <prompt_certificate>0</prompt_certificate>
                            <server>ipsec.fortinet.com</server>
                            <authentication_method>Preshared
Key</authentication_method>
                            <auth_key>Enc
ce9b42bb02f08b362a62f9a230730c3ac2282f11d3403c75b4f8f2df28ca274d</auth_key>
                            <mode>aggressive</mode>
                            <dhgroup>5;</dhgroup>
                            <key_life>28800</key_life>
                            <localid></localid>
                            <nat_traversal>1</nat_traversal>
                            <mode_config>1</mode_config>
                            <enable_local_lan>0</enable_local_lan>
                            <nat_alive_freq>5</nat_alive_freq>
                            <dpd>1</dpd>
                            <dpd_retry_count>3</dpd_retry_count>
                            <dpd_retry_interval>5</dpd_retry_interval>
                            <enable_ike_fragmentation>0</enable_ike_fragmentation>
                            <xauth>
                                <enabled>1</enabled>
                                <prompt_username>1</prompt_username>
                                <username>Enc
a5766c404fa3b692a948f5e50b8cbeb9decf9a418d0cc9bd187320f814a06e1e0a5a</username
>
                                <password />
                            </xauth>
                            <proposals>
                                <proposal>3DES|MD5</proposal>
                                <proposal>3DES|SHA1</proposal>
                                <proposal>AES128|MD5</proposal>
                                <proposal>AES128|SHA1</proposal>
                            </proposals>
                        </ike_settings>
                        <ipsec_settings>
                            <remote_networks>
                                <network>
                                    <addr>0.0.0.0</addr>
                                    <mask>0.0.0.0</mask>
                                </network>
                            </remote_networks>
```

```
                        <dhgroup>5</dhgroup>
                        <key_life_type>seconds</key_life_type>
                        <key_life_seconds>1800</key_life_seconds>
                        <key_life_Kbytes>5120</key_life_Kbytes>
                        <replay_detection>1</replay_detection>
                        <pfs>1</pfs>
                        <autokey_keep_alive>0</autokey_keep_alive>
                        <use_vip>1</use_vip>
                        <virtualip>
                            <type>modeconfig</type>
                            <ip>0.0.0.0</ip>
                            <mask>0.0.0.0</mask>
                            <dnsserver>0.0.0.0</dnsserver>
                            <winserver>0.0.0.0</winserver>
                        </virtualip>
                        <proposals>
                            <proposal>3DES|MD5</proposal>
                            <proposal>3DES|SHA1</proposal>
                            <proposal>AES128|MD5</proposal>
                            <proposal>AES128|SHA1</proposal>
                        </proposals>
                    </ipsec_settings>
                    <on_connect>
                        <script>
                            <os>windows</os>
                            <script>
                                <!--Write MS DOS batch script inside the CDATA
tag below.
One line per command, just like a regular batch script file.
The script will be executed in the context of the user that connected the
tunnel.
Wherever you write #username# in your script, it will be automatically
substituted with the xauth username of the user that connected the tunnel.
Wherever you write #password# in your script, it will be automatically
substituted with the xauth password of the user that connected the tunnel.
Remember to check your xml file before deploying to ensure that carriage
returns/line feeds are present.
-->
                                <script>
                                    <![CDATA[
mkdir %temp%\jose
]]></script>
                            </script>
                        </script>
                    </on_connect>
                    <on_disconnect>
                        <script>
```

```
                            <os>windows</os>
                            <script>
                                <!--Write MS DOS batch script inside the CDATA
tag below.
One line per command, just like a regular batch script file.
The script will be executed in the context of the user that connected the
tunnel.
Wherever you write #username# in your script, it will be automatically
substituted with the xauth username of the user that connected the tunnel.
Wherever you write #password# in your script, it will be automatically
substituted with the xauth password of the user that connected the tunnel.
Remember to check your xml file before deploying to ensure that carriage
returns/line feeds are present.
-->
                                <script>
                                    <![CDATA[
rmdir %temp%\jose
]]></script>
                            </script>
                        </script>
                    </on_disconnect>
                </connection>
            </connections>
        </ipsecvpn>
    </vpn>
    <certificates>
        <crl>
            <ocsp />
        </crl>
    </certificates>
    <antivirus>
        <signature_expired_notification>0</signature_expired_notification>
        <scan_on_insertion>0</scan_on_insertion>
        <shell_integration>1</shell_integration>
        <antirootkit>4294967295</antirootkit>
        <fortiguard_analytics>1</fortiguard_analytics>
        <multi_process_limit>0</multi_process_limit>
        <scheduled_scans>
            <!--zero, one or more of the following child nodes-->
            <full>
                <enabled>1</enabled>
                <repeat>1</repeat>
                <days>2</days>
                <time>18:30</time>
                <removable_media>1</removable_media>
                <network_drives>0</network_drives>
                <priority>0</priority>
```

```
            </full>
        </scheduled_scans>
        <on_demand_scanning>
            <on_virus_found>0</on_virus_found>
            <pause_on_battery_power>1</pause_on_battery_power>
            <automatic_virus_submission>
                <enabled>0</enabled>
                <smtp_server>fortinetvirussubmit.com</smtp_server>
                <username />
                <password>Enc
56336028ce9daca3a4e63bad972bbbe9455de5803b3be8ea</password>
            </automatic_virus_submission>
            <compressed_files>
                <scan>1</scan>
                <maxsize>0</maxsize>
            </compressed_files>
            <riskware>
                <enabled>1</enabled>
            </riskware>
            <adware>
                <enabled>1</enabled>
            </adware>
            <heuristic_scanning>0</heuristic_scanning>
            <scan_file_types>
                <all_files>1</all_files>
                <file_types>

<extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.ASX,.AVB,.AX,.AX2,.B
AT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CS
H,.CSS,.DEV,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.GVB,.HLP,.HTA,.
HTM,.HTML,.HTT,.HTW,.HTX,.HXS,.INF,.INI,.JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB
,.MHT,.MHTM,.MHTML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PNF,.PNP,.
POT,.PPA,.PPS,.PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.RTF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,
.SHT,.SHTML,.SHW,.SIS,.SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS,.
VBX,.VOM,.VSD,.VSS,.VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WIZ,.WK,.WML,.WPC,.WPD,.WSC,
.WSF,.WSH,.XLS,.XML,.XTP</extensions>

<include_files_with_no_extension>0</include_files_with_no_extension>
                </file_types>
            </scan_file_types>
            <exclusions>
                <!--the element below can exist 0-n times-->
                <!--the element below can exist 0-n times-->
                <file_types>
                    <extensions />
                </file_types>
            </exclusions>
        </on_demand_scanning>
```

```
            <real_time_protection>
                <enabled>1</enabled>
                <when>0</when>
                <on_virus_found>5</on_virus_found>
                <popup_alerts>1</popup_alerts>
                <popup_registry_alerts>0</popup_registry_alerts>
                <compressed_files>
                    <scan>1</scan>
                    <maxsize>10</maxsize>
                </compressed_files>
                <riskware>
                    <enabled>1</enabled>
                </riskware>
                <adware>
                    <enabled>1</enabled>
                </adware>
                <heuristic_scanning>
                    <enabled>0</enabled>
                    <action>3</action>
                </heuristic_scanning>
                <scan_file_types>
                    <all_files>0</all_files>
                    <file_types>

<extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.ASX,.AVB,.AX,.AX2,.B
AT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CS
H,.CSS,.DEV,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.GVB,.HLP,.HTA,.
HTM,.HTML,.HTT,.HTW,.HTX,.HXS,.INF,.INI,.JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB
,.MHT,.MHTM,.MHTML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PNF,.PNP,.
POT,.PPA,.PPS,.PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.RTF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,
.SHT,.SHTML,.SHW,.SIS,.SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS,.
VBX,.VOM,.VSD,.VSS,.VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WIZ,.WK,.WML,.WPC,.WPD,.WSC,
.WSF,.WSH,.XLS,.XML,.XTP</extensions>

<include_files_with_no_extension>0</include_files_with_no_extension>
                    </file_types>
                </scan_file_types>
                <exclusions>
                    <!--the element below can exist 0-n times-->
                    <!--the element below can exist 0-n times-->
                    <file_types>
                        <extensions />
                    </file_types>
                </exclusions>
            </real_time_protection>
            <email>
                <smtp>1</smtp>
                <pop3>1</pop3>
```

```
                <outlook>1</outlook>
                <wormdetection>
                    <enabled>0</enabled>
                    <action>0</action>
                </wormdetection>
                <heuristic_scanning>
                    <enabled>0</enabled>
                    <action>0</action>
                </heuristic_scanning>
            </email>
            <quarantine>
                <cullage>100</cullage>
            </quarantine>
            <server>
                <exchange>
                    <integrate>0</integrate>
                    <action>0</action>
                   <excludefilesystemfromscanning>0</excludefilesystemfromscanning>

<excludefileextensionsfromscanning>0</excludefileextensionsfromscanning>
                </exchange>
                <sqlserver>
                   <excludefilesystemfromscanning>0</excludefilesystemfromscanning>

<excludefileextensionsfromscanning>0</excludefileextensionsfromscanning>
                </sqlserver>
            </server>
        </antivirus>
        <endpoint_control>
            <enabled>1</enabled>
            <!--short keepalive timeout in ms-->
            <keepalive_short_timeout>20000</keepalive_short_timeout>
            <!--keepalive timeout in seconds-->
            <keepalive_timeout>1800</keepalive_timeout>
            <custom_ping_server />
            <ping_server>172.17.61.178:8010</ping_server>
            <fgt_name>al-fwf81cm</fgt_name>
            <fgt_sn>Enc
38f4de3b057be8b23284ec0d0c335fe82eb06ffd05bc65f8291b33d8c42f484287d76d19df50eb
57a82c397bbe3ddcf32bd08d5abf5de4c0db98feb22614e28d09d582d79ccc9cf03a028222e2f2
c460779f0b7c5ad0a0dd84</fgt_sn>
            <offnet_update>1</offnet_update>
            <user>Enc 6e9856c6749d579e3cecb04d3ec939cc5b9fe50c274b5c75cbfa</user>
            <skip_confirmation>0</skip_confirmation>
            <conf_recv_time>1371494178</conf_recv_time>
            <vdom>root</vdom>
            <disable_unregister>0</disable_unregister>
```

```
        <show_bubble_notifications>1</show_bubble_notifications>
        <fgt_list>Enc
7dae0017faca16e4d1518df60f999ec48264183c080782dc3e27c0d420f6ce5087badccc8fce2e
1113b6d875ac8c6241aedd5b2024c3b5a6a8e7ea5633ec9f38b8d805cbce2b578e5f55996da456
034a7abebc21d6a0e3aa83a9793f</fgt_list>
        <ui>
            <display_antivirus>1</display_antivirus>
            <display_webfilter>1</display_webfilter>
            <display_firewall>1</display_firewall>
            <display_vpn>1</display_vpn>
            <display_vulnerability_scan>1</display_vulnerability_scan>
            <registration_dialog>
                <show_profile_details>1</show_profile_details>
            </registration_dialog>
        </ui>
        <fortigates>
            <fortigate>
                <serial_number />
                <name />
                <registration_password />
                <addresses />
            </fortigate>
        </fortigates>
    </endpoint_control>
    <fssoma>
        <enabled>0</enabled>
        <serveraddress />
        <presharedkey>Enc
60837be73aab6a596dc5b3e40b3d77c023a663b96586f152</presharedkey>
    </fssoma>
    <wan_optimization>
        <enabled>0</enabled>
        <support_http>1</support_http>
        <support_cifs>1</support_cifs>
        <support_mapi>1</support_mapi>
        <support_ftp>1</support_ftp>
        <max_disk_cache_size_mb>512</max_disk_cache_size_mb>
    </wan_optimization>
    <webfilter>
        <https_enabled>1</https_enabled>
        <!--use enable_filter to enable/disable WebFiltering-->
        <enable_filter>1</enable_filter>
        <!--enabled enables/disables the FortiGuard querying service.-->
        <enabled>1</enabled>
        <log_all_urls>0</log_all_urls>
        <white_list_has_priority>0</white_list_has_priority>
        <current_profile>1000</current_profile>
```

```
<partial_match_host>0</partial_match_host>
<disable_when_managed>0</disable_when_managed>
<max_violations>5000</max_violations>
<max_violation_age>90</max_violation_age>
<fortiguard>
    <enabled>1</enabled>
    <rate_ip_addresses>0</rate_ip_addresses>
</fortiguard>
<profiles>
    <profile>
        <id>1000</id>
        <cate_ver>6</cate_ver>
        <description />
        <name />
        <temp_whitelist_timeout>300</temp_whitelist_timeout>
        <categories>
            <category>
                <id>0
                    <!--Unrated (Unrated)-->
                </id>
                <action>warn</action>
            </category>
            <category>
                <id>2
                    <!--Alternative Beliefs (Adult/Mature Content)-->
                </id>
                <action>warn</action>
            </category>
            <category>
                <id>7
                    <!--Abortion (Adult/Mature Content)-->
                </id>
                <action>warn</action>
            </category>
            <category>
                <id>8
                    <!--Other Adult Materials (Adult/Mature Content)-->
                </id>
                <action>warn</action>
            </category>
            <category>
                <id>9
                   <!--Advocacy Organizations (Adult/Mature Content)-->
                </id>
                <action>warn</action>
            </category>
```

```
<category>
    <id>11
        <!--Gambling (Adult/Mature Content)-->
    </id>
    <action>warn</action>
</category>
<category>
    <id>12
        <!--Extremist Groups (Potentially Liable)-->
    </id>
    <action>warn</action>
</category>
<category>
    <id>13
        <!--Nudity and Risque (Adult/Mature Content)-->
    </id>
    <action>warn</action>
</category>
<category>
    <id>14
        <!--Pornography (Adult/Mature Content)-->
    </id>
    <action>warn</action>
</category>
<category>
    <id>15
        <!--Dating (Adult/Mature Content)-->
    </id>
    <action>warn</action>
</category>
<category>
    <id>16
        <!--Weapons (Sales) (Adult/Mature Content)-->
    </id>
    <action>warn</action>
</category>
<category>
    <id>26
        <!--Malicious Websites (Security Risk)-->
    </id>
    <action>deny</action>
</category>
<category>
    <id>57
        <!--Marijuana (Adult/Mature Content)-->
    </id>
```

```
                        <action>warn</action>
                    </category>
                    <category>
                        <id>63
                            <!--Sex Education (Adult/Mature Content)-->
                        </id>
                        <action>warn</action>
                    </category>
                    <category>
                        <id>64
                            <!--Alcohol (Adult/Mature Content)-->
                        </id>
                        <action>warn</action>
                    </category>
                    <category>
                        <id>65
                            <!--Tobacco (Adult/Mature Content)-->
                        </id>
                        <action>warn</action>
                    </category>
                    <category>
                        <id>66
                            <!--Lingerie and Swimsuit (Adult/Mature Content)-->
                        </id>
                        <action>warn</action>
                    </category>
                    <category>
                        <id>67
                            <!--Sports Hunting and War Games (Adult/Mature
Content)-->
                        </id>
                        <action>warn</action>
                    </category>
                </categories>
                <safe_search>
                    <enabled>0</enabled>
                    <search_engines>
                        <enabled>1</enabled>
                        <engine>
                            <name>Bing</name>
                            <host>
                                <![CDATA[www\.bing\.com]]></host>
                            <url>

<![CDATA[^(\/images|\/videos)?(\/search|\/async)\?]]></url>
                            <query>
```

```
                                <![CDATA[q=]]></query>
                            <safe_search_string>
                                <![CDATA[&adlt=strict]]></safe_search_string>
                            <cookie_name>SRCHHPGUSR</cookie_name>
                            <cookie_value>
                                <![CDATA[adlt=strict]]></cookie_value>
                        </engine>
                        <engine>
                            <name>Google</name>
                            <host>
                                <![CDATA[.*\.google\..*]]></host>
                            <url>

<![CDATA[^\/((custom|search|images|videosearch|webhp)\?)]]></url>
                            <query>
                                <![CDATA[q=]]></query>
                            <safe_search_string>
                                <![CDATA[&safe=active]]></safe_search_string>
                        </engine>
                        <engine>
                            <name>Yahoo</name>
                            <host>
                                <![CDATA[.*\.yahoo\..*]]></host>
                            <url>

<![CDATA[^\/search(\/video|\/images){0,1}(\?|;)]]></url>
                            <query>
                                <![CDATA[p=]]></query>
                            <safe_search_string>
                                <![CDATA[&vm=r]]></safe_search_string>
                        </engine>
                        <engine>
                            <name>Yandex</name>
                            <host>
                                <![CDATA[yandex\..*]]></host>
                            <url>

<![CDATA[^\/(yand){0,1}(search)[/]{0,}.{0,}\?]]></url>
                            <query>
                                <![CDATA[text=]]></query>
                            <safe_search_string>
                                <![CDATA[&fyandex=1]]></safe_search_string>
                        </engine>
                        <engine>
                            <name>YouTube</name>
                            <host>
```

```
                                <![CDATA[.*\.youtube\..*]]></host>
                            <cookie_name>PREF</cookie_name>
                            <cookie_value>
                                <![CDATA[f2=8000000]]></cookie_value>
                        </engine>
                    </search_engines>
                    <youtube_education_filter>
                        <enabled>0</enabled>
                        <filter_id>
                            <![CDATA[]]></filter_id>
                    </youtube_education_filter>
                </safe_search>
            </profile>
            <!--
This is a table of all Web Filter categories (Id ==> Category Name)
0 ==> Unrated
1 ==> Drug Abuse
2 ==> Alternative Beliefs
3 ==> Hacking
4 ==> Illegal or Unethical
5 ==> Discrimination
6 ==> Explicit Violence
7 ==> Abortion
8 ==> Other Adult Materials
9 ==> Advocacy Organizations
11 ==> Gambling
12 ==> Extremist Groups
13 ==> Nudity and Risque
14 ==> Pornography
15 ==> Dating
16 ==> Weapons (Sales)
17 ==> Advertising
18 ==> Brokerage and Trading
19 ==> Freeware and Software Downloads
20 ==> Games
23 ==> Web-based Email
24 ==> File Sharing and Storage
25 ==> Streaming Media and Download
26 ==> Malicious Websites
28 ==> Entertainment
29 ==> Arts and Culture
30 ==> Education
31 ==> Finance and Banking
33 ==> Health and Wellness
34 ==> Job Search
35 ==> Medicine
```

```
36 ==> News and Media
37 ==> Social Networking
38 ==> Political Organizations
39 ==> Reference
40 ==> Global Religion
41 ==> Search Engines and Portals
42 ==> Shopping and Auction
43 ==> General Organizations
44 ==> Society and Lifestyles
46 ==> Sports
47 ==> Travel
48 ==> Personal Vehicles
49 ==> Business
50 ==> Information and Computer Security
51 ==> Government and Legal Organizations
52 ==> Information Technology
53 ==> Armed Forces
54 ==> Dynamic Content
55 ==> Meaningless Content
56 ==> Web Hosting
57 ==> Marijuana
58 ==> Folklore
59 ==> Proxy Avoidance
61 ==> Phishing
62 ==> Plagiarism
63 ==> Sex Education
64 ==> Alcohol
65 ==> Tobacco
66 ==> Lingerie and Swimsuit
67 ==> Sports Hunting and War Games
68 ==> Web Chat
69 ==> Instant Messaging
70 ==> Newsgroups and Message Boards
71 ==> Digital Postcards
72 ==> Peer-to-peer File Sharing
75 ==> Internet Radio and TV
76 ==> Internet Telephony
77 ==> Child Education
78 ==> Real Estate
79 ==> Restaurant and Dining
80 ==> Personal Websites and Blogs
81 ==> Secure Websites
82 ==> Content Servers
83 ==> Child Abuse
84 ==> Web-based Applications
85 ==> Domain Parking
```

```
86 ==> Spam URLs
87 ==> Personal Privacy
-->
        </profiles>
    </webfilter>
    <firewall>
        <enabled>1</enabled>
        <current_profile>1000</current_profile>
        <default_action>Pass</default_action>
        <show_bubble_notifications>1</show_bubble_notifications>
        <max_violations>5000</max_violations>
        <max_violation_age>90</max_violation_age>
        <profiles>
            <profile>
                <id>0</id>
                <rules>
                    <rule>
                        <action>Block</action>
                        <enabled>1</enabled>
                        <category>
                            <id>19</id>
                            <!--Botnet-->
                        </category>
                    </rule>
                </rules>
            </profile>
            <profile>
                <id>1000</id>
                <rules>
                    <rule>
                        <action>Pass</action>
                        <enabled>1</enabled>
                        <category>
                            <id>2</id>
                            <!--P2P-->
                        </category>
                        <behavior>
                            <id>All</id>
                            <!--P2P-->
                        </behavior>
                        <technology>
                            <id>All</id>
                            <!--P2P-->
                        </technology>
                        <vendor>
                            <id>All</id>
```

```
                        <!--P2P-->
                    </vendor>
                    <protocol>
                        <id>All</id>
                        <!--P2P-->
                    </protocol>
                </rule>
                <rule>
                    <action>Pass</action>
                    <enabled>1</enabled>
                    <category>
                        <id>5</id>
                        <!--Video/Audio-->
                    </category>
                    <behavior>
                        <id>All</id>
                        <!--Video/Audio-->
                    </behavior>
                    <technology>
                        <id>All</id>
                        <!--Video/Audio-->
                    </technology>
                    <vendor>
                        <id>All</id>
                        <!--Video/Audio-->
                    </vendor>
                    <protocol>
                        <id>All</id>
                        <!--Video/Audio-->
                    </protocol>
                </rule>
                <rule>
                    <action>Pass</action>
                    <enabled>1</enabled>
                    <application>
                        <id>All</id>
                        <!--All Known Applications-->
                    </application>
                </rule>
            </rules>
        </profile>
        <!--
This is a table of all Application Firewall categories (Id ==> Category Name)
-->
    </profiles>
</firewall>
```

```
    <vulnerability_scan>
        <enabled>1</enabled>
        <scheduled_scans>
            <schedule>
                <repeat>0</repeat>
                <type>24</type>
                <time>11:35</time>
            </schedule>
        </scheduled_scans>
    </vulnerability_scan>
</forticlient_configuration>
```

Example FortiClient XML configuration file (Mac OS X)

The following is an example FortiClient XML configuration file. VPN autoconnect and always up are enabled in the configuration.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<forticlient_configuration>
    <forticlient_version>5.0.5.0127</forticlient_version>
    <version>5.0</version>
    <date>2013-08-08</date>
    <os_version>MacOSX</os_version>
    <partial_configuration>0</partial_configuration>
    <system>
        <log_settings>
            <level>1</level>
            <max_log_size>10000000</max_log_size>

<log_events>ipsecvpn,sslvpn,webfilter,update,av,firewall</log_events>
            <remote_logging>
                <log_upload_enabled>0</log_upload_enabled>
                <log_upload_server></log_upload_server>
                <log_upload_freq_hours>0</log_upload_freq_hours>
                <log_upload_ssl_enabled>0</log_upload_ssl_enabled>
                <netlog_categories>7</netlog_categories>
                <log_retention_days>90</log_retention_days>
            </remote_logging>
        </log_settings>
        <proxy>
            <address></address>
            <port></port>
            <username></username>
            <password></password>
            <update></update>
        </proxy>
        <update>
            <use_custom_server>0</use_custom_server>
            <server></server>
            <port></port>
            <failoverport></failoverport>
            <fail_over_to_fdn>1</fail_over_to_fdn>
            <fail_over_servers></fail_over_servers>
            <update_action>notify_only</update_action>
            <scheduled_update>
                <enabled>1</enabled>
                <type>interval</type>
```

```
                <update_interval_in_hours>3</update_interval_in_hours>
            </scheduled_update>
        </update>
        <ui>
            <password>Enc
420d2ee65abded897a69c50f4995397969f1c1f949055d8e51</password>
            <default_tab>AV</default_tab>
            <culture_code></culture_code>
            <ads>1</ads>
        </ui>
    </system>
    <vpn>
        <options>
            <autoconnect_tunnel></autoconnect_tunnel>
            <keep_running_max_retries>0</keep_running_max_retries>
            <allow_personal_vpns>1</allow_personal_vpns>
        </options>
        <ipsecvpn>
            <options>
                <enabled>1</enabled>
            </options>
            <connections>
                <connection>
                    <name>IPSec</name>
                    <type>manual</type>
                    <ike_settings>
                        <prompt_certificate>0</prompt_certificate>
                        <description></description>
                        <server>ipsec.fortinet.com</server>
                        <authentication_method>Preshared
Key</authentication_method>
                        <auth_key>Enc
420d2ee65abded897a69c50f49950859b45c780adb269f3aa69aaa6690d2984032</auth_key>
                        <mode>aggressive</mode>
                        <dhgroup>5</dhgroup>
                        <key_life>28800</key_life>
                        <localid></localid>
                        <nat_traversal>1</nat_traversal>
                        <mode_config>1</mode_config>
                        <dpd>1</dpd>
                        <xauth>
                            <enabled>1</enabled>
                            <prompt_username>0</prompt_username>
```

```
                        <username>Enc
420d2ee65abded897a69c50f49957307f6086969836dfef7acb9235e939b584d80877a</userna
me>
                        <password>Enc
420d2ee65abded897a69c50f4995397969f1c1f949055d8e51</password>
                    </xauth>
                    <proposals>
                        <proposal>3des|md5</proposal>
                        <proposal>3des|sha1</proposal>
                        <proposal>aes128|md5</proposal>
                        <proposal>aes128|sha1</proposal>
                        <proposal>aes256|md5</proposal>
                        <proposal>aes256|sha1</proposal>
                        <proposal>aes|md5</proposal>
                        <proposal>aes|sha1</proposal>
                        <proposal>des|md5</proposal>
                        <proposal>des|sha1</proposal>
                    </proposals>
                    <fgt>0</fgt>
                </ike_settings>
                <ipsec_settings>
                    <remote_networks></remote_networks>
                    <dhgroup>5</dhgroup>
                    <key_life_type>seconds</key_life_type>
                    <key_life_seconds>1800</key_life_seconds>
                    <pfs></pfs>
                    <use_vip>1</use_vip>
                    <virtualip>
                        <type>modeconfig</type>
                        <ip></ip>
                        <mask></mask>
                        <dnsserver></dnsserver>
                    </virtualip>
                    <proposals></proposals>
                </ipsec_settings>
                <on_connect>
                    <script>
                        <os>mac</os>
                        <script>mkdir /tmp/jose</script>
                    </script>
                </on_connect>
                <on_disconnect>
                    <script>
                        <os>mac</os>
```

```
                            <script>rmdir /tmp/jose</script>
                        </script>
                    </on_disconnect>
                    <keep_running>0</keep_running>
                    <ui>
                        <show_passcode>0</show_passcode>
                        <show_remember_password>0</show_remember_password>
                        <show_alwaysup>0</show_alwaysup>
                        <show_autoconnect>0</show_autoconnect>
                    </ui>
                </connection>
            </connections>
        </ipsecvpn>
        <sslvpn>
            <options>
                <enabled>1</enabled>
            </options>
            <connections>
                <connection>
                    <name>SSL</name>
                    <description></description>
                    <server>ssl.fortinet.com:443</server>
                    <username>Enc
420d2ee65abded897a69c50f49957307f6086969836dfef7acb9235e939b584d80877a</userna
me>
                    <password>Enc
420d2ee65abded897a69c50f4995397969f1c1f949055d8e51</password>
                    <certificate>Enc
420d2ee65abded897a69c50f4995397969f1c1f949055d8e51</certificate>

<warn_invalid_server_certificate>1</warn_invalid_server_certificate>
                    <prompt_certificate>0</prompt_certificate>
                    <prompt_username>0</prompt_username>
                    <on_connect>
                        <script>
                            <os>mac</os>
                            <script>mkdir /tmp/jose</script>
                        </script>
                    </on_connect>
                    <on_disconnect>
                        <script>
                            <os>mac</os>
                            <script>rmdir /tmp/jose</script>
                        </script>
```

```
                    </on_disconnect>
                    <keep_running>0</keep_running>
                    <fgt>0</fgt>
                    <ui>
                        <show_remember_password>0</show_remember_password>
                        <show_alwaysup>0</show_alwaysup>
                        <show_autoconnect>0</show_autoconnect>
                    </ui>
                </connection>
            </connections>
        </sslvpn>
    </vpn>
    <endpoint_control>
        <enable_enforcement></enable_enforcement>
        <enabled>1</enabled>
        <keepalive_short_timeout>300</keepalive_short_timeout>
        <collect_app_statistics></collect_app_statistics>
        <fgt_name>al-fwf81cm</fgt_name>
        <fgt_sn>Enc
420d2ee65abded897a69c50f49957a50c15d0c0adc21aed99c3ff9a0b82e25b436e9f71fa4c793
c76cca9fe99a0228c878fe8b0a329a0c1daf89aa9ccae388a40bc83d755076c3dcdc61d6f78501
f1a247264f8b2bb67d361104</fgt_sn>
        <checksum></checksum>
        <corporate_id>Enc
420d2ee65abded897a69c50f49957c06e64d7d09da73adfec94bf9f9ea7a799337e98339a9e1ca
ca6abdefe89e7372e849a48d2b1c99044eab89a1efc2948fda08cc38712676b9d8d761ddf7ff01
f1e3c70d64ffa17f3fb83503a0573af877598d852018782e</corporate_id>
        <ping_server>172.17.61.178:8010</ping_server>
        <custom_ping_server>:0</custom_ping_server>
        <log_last_upload_date>0</log_last_upload_date>
        <conf_recv_time>1371494514</conf_recv_time>
        <fgt_logoff_on_fct_shutdown>1</fgt_logoff_on_fct_shutdown>
        <offnet_update>1</offnet_update>
        <fgt_list>Enc
420d2ee65abded897a69c50f49957f3fbd5c0a76d92eaea99a4dfca8bb29609663fdd02afbbd9a
9d33f5efea986822b901f08b674e9e0d50a58fab9c8695d1fc19ce3c7000749e88d9648cacd85d
ac9abc0142f3fc2f1a9f3503806e2cc2cf244708664842440584a372d4c09dd570d8e1780a19bf
3a447690d678dd227bebc8cb349f0a1c8575674fc4cf52c6b50e845cc39ff1261eb68fdc0d539b
dc09c7a1c63bba9578c57991117a7f8da92d40d92f8f9b7da248b640a6fcf675bdb130d3241a83
0f37f8642975d6102269e13415a0e2ba58bd2600a5d80d79bc2e4a681a</fgt_list>
        <fortigates></fortigates>
        <ui>
            <display_antivirus>1</display_antivirus>
            <display_webfilter>1</display_webfilter>
            <display_firewall>1</display_firewall>
            <display_vpn>1</display_vpn>
```

```
            <display_vulnerability_scan>1</display_vulnerability_scan>
        </ui>
        <silent_registration>0</silent_registration>
        <vdom>root</vdom>
    </endpoint_control>
    <webfilter>
        <enable_filter>1</enable_filter>
        <disable_when_managed>0</disable_when_managed>
        <enabled>1</enabled>
        <current_profile>1000</current_profile>
        <log_all_urls>0</log_all_urls>
        <white_list_has_priority>0</white_list_has_priority>
        <partial_match_host>1</partial_match_host>
        <fortiguard>
            <enabled>0</enabled>
            <rate_ip_addresses>0</rate_ip_addresses>
        </fortiguard>
        <show_bubble_notifications>0</show_bubble_notifications>
        <profiles>
            <profile>
                <id>0</id>
                <display_name>Default Profile</display_name>
                <description></description>
                <cate_ver>6</cate_ver>
                <categories>
                    <category>
                        <id>1</id>
                        <action>deny</action>
                    </category>
                    <category>
                        <id>2</id>
                        <action>deny</action>
                    </category>
                    <category>
                        <id>3</id>
                        <action>deny</action>
                    </category>
                    <category>
                        <id>4</id>
                        <action>deny</action>
                    </category>
                    <category>
                        <id>5</id>
```

```
        <action>deny</action>
    </category>
    <category>
        <id>6</id>
        <action>deny</action>
    </category>
    <category>
        <id>7</id>
        <action>deny</action>
    </category>
    <category>
        <id>8</id>
        <action>deny</action>
    </category>
    <category>
        <id>9</id>
        <action>deny</action>
    </category>
    <category>
        <id>11</id>
        <action>deny</action>
    </category>
    <category>
        <id>12</id>
        <action>deny</action>
    </category>
    <category>
        <id>13</id>
        <action>deny</action>
    </category>
    <category>
        <id>14</id>
        <action>deny</action>
    </category>
    <category>
        <id>15</id>
        <action>deny</action>
    </category>
    <category>
        <id>16</id>
        <action>deny</action>
    </category>
    <category>
```

```
                <id>26</id>
                <action>deny</action>
            </category>
            <category>
                <id>57</id>
                <action>deny</action>
            </category>
            <category>
                <id>59</id>
                <action>deny</action>
            </category>
            <category>
                <id>61</id>
                <action>deny</action>
            </category>
            <category>
                <id>62</id>
                <action>deny</action>
            </category>
            <category>
                <id>64</id>
                <action>deny</action>
            </category>
            <category>
                <id>65</id>
                <action>deny</action>
            </category>
            <category>
                <id>83</id>
                <action>deny</action>
            </category>
            <category>
                <id>86</id>
                <action>deny</action>
            </category>
        </categories>
        <urls></urls>
        <safe_search>
            <enabled>0</enabled>
            <youtube_education_filter>
                <enabled>0</enabled>
                <filter_id></filter_id>
            </youtube_education_filter>
```

```
            <search_engines>
                <enabled>0</enabled>
            </search_engines>
        </safe_search>
    </profile>
    <profile>
        <id>1000</id>
        <display_name>1000</display_name>
        <description></description>
        <cate_ver>0</cate_ver>
        <categories>
            <category>
                <id>0</id>
                <action>monitor</action>
            </category>
            <category>
                <id>2</id>
                <action>monitor</action>
            </category>
            <category>
                <id>7</id>
                <action>monitor</action>
            </category>
            <category>
                <id>8</id>
                <action>monitor</action>
            </category>
            <category>
                <id>9</id>
                <action>monitor</action>
            </category>
            <category>
                <id>11</id>
                <action>monitor</action>
            </category>
            <category>
                <id>12</id>
                <action>monitor</action>
            </category>
            <category>
                <id>13</id>
                <action>monitor</action>
            </category>
```

```
            <category>
                <id>14</id>
                <action>monitor</action>
            </category>
            <category>
                <id>15</id>
                <action>monitor</action>
            </category>
            <category>
                <id>16</id>
                <action>monitor</action>
            </category>
            <category>
                <id>26</id>
                <action>deny</action>
            </category>
            <category>
                <id>57</id>
                <action>monitor</action>
            </category>
            <category>
                <id>63</id>
                <action>monitor</action>
            </category>
            <category>
                <id>64</id>
                <action>monitor</action>
            </category>
            <category>
                <id>65</id>
                <action>monitor</action>
            </category>
            <category>
                <id>66</id>
                <action>monitor</action>
            </category>
            <category>
                <id>67</id>
                <action>monitor</action>
            </category>
        </categories>
        <urls></urls>
        <safe_search>
```

```
                <enabled>0</enabled>
                <youtube_education_filter>
                    <enabled>0</enabled>
                    <filter_id></filter_id>
                </youtube_education_filter>
                <search_engines>
                    <enabled>0</enabled>
                </search_engines>
            </safe_search>
        </profile>
    </profiles>
</webfilter>
<firewall>
    <enabled>1</enabled>
    <show_bubble_notifications>1</show_bubble_notifications>
    <current_profile>1000</current_profile>
    <profiles>
        <profile>
            <id>0</id>
            <rules>
                <rule>
                    <id></id>
                    <filter>
                        <category>19</category>
                        <vendor></vendor>
                        <behavior></behavior>
                        <technology></technology>
                        <protocol></protocol>
                        <application></application>
                        <popularity></popularity>
                    </filter>
                    <action>block</action>
                    <enabled>1</enabled>
                </rule>
            </rules>
        </profile>
        <profile>
            <id>1000</id>
            <rules>
                <rule>
                    <id></id>
                    <filter>
                        <category>2</category>
```

```
                        <vendor>All</vendor>
                        <behavior>All</behavior>
                        <technology>All</technology>
                        <protocol>All</protocol>
                        <application></application>
                        <popularity></popularity>
                    </filter>
                    <action>pass</action>
                    <enabled>1</enabled>
                </rule>
                <rule>
                    <id></id>
                    <filter>
                        <category>5</category>
                        <vendor>All</vendor>
                        <behavior>All</behavior>
                        <technology>All</technology>
                        <protocol>All</protocol>
                        <application></application>
                        <popularity></popularity>
                    </filter>
                    <action>pass</action>
                    <enabled>1</enabled>
                </rule>
                <rule>
                    <id></id>
                    <filter>
                        <category></category>
                        <vendor></vendor>
                        <behavior></behavior>
                        <technology></technology>
                        <protocol></protocol>
                        <application>All</application>
                        <popularity></popularity>
                    </filter>
                    <action>pass</action>
                    <enabled>1</enabled>
                </rule>
            </rules>
        </profile>
    </profiles>
</firewall>
<vulnerability_scan>
```

```
        <enabled>1</enabled>
        <scan_on_fgt_registration>0</scan_on_fgt_registration>
        <scheduled_scans>
            <schedule>
                <repeat>0</repeat>
                <type>24</type>
                <day>0</day>
                <time>11:39:54</time>
            </schedule>
        </scheduled_scans>
    </vulnerability_scan>
    <antivirus>
        <scheduled_scans>
            <full>
                <enabled>1</enabled>
                <repeat>1</repeat>
                <days>2</days>
                <time>18:30</time>
                <removable_media>1</removable_media>
            </full>
        </scheduled_scans>
        <on_demand_scanning>
            <on_virus_found>4</on_virus_found>
            <compressed_files>
                <scan>1</scan>
                <maxsize>0</maxsize>
            </compressed_files>
            <riskware>
                <enabled>0</enabled>
            </riskware>
            <adware>
                <enabled>0</enabled>
            </adware>
            <heuristic_scanning>0</heuristic_scanning>
            <exclusions></exclusions>
        </on_demand_scanning>
        <real_time_protection>
            <enabled>1</enabled>
            <when>0</when>
            <on_virus_found>5</on_virus_found>
            <popup_alerts>1</popup_alerts>
            <compressed_files>
                <scan>1</scan>
```

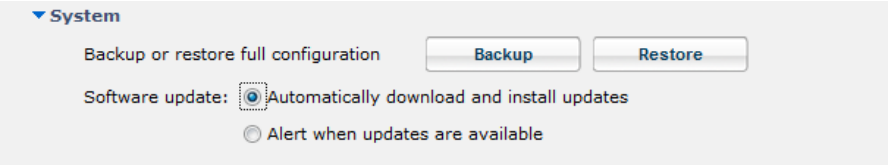
```
                <maxsize>2</maxsize>
            </compressed_files>
            <riskware>
                <enabled>0</enabled>
            </riskware>
            <adware>
                <enabled>0</enabled>
            </adware>
            <heuristic_scanning>
                <enabled>0</enabled>
                <action>0</action>
            </heuristic_scanning>
            <exclusions></exclusions>
        </real_time_protection>
        <quarantine>
            <cullage>100</cullage>
        </quarantine>
    </antivirus>
</forticlient_configuration>
```

Backup or Restore the Configuration File

Backup the full configuration file

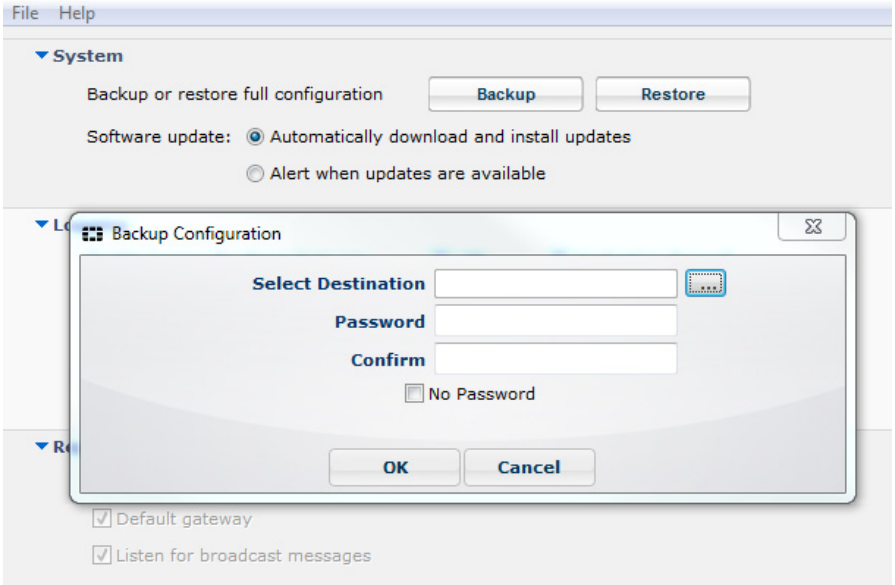
To backup the full configuration file, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *System* to view the drop-down menu. On this menu you can perform a backup of the full configuration file.

Figure 1: Backup and Restore options



When performing a backup, you can select the file destination, and save the file in an unencrypted or encrypted format. To encrypt the configuration file enter a password.

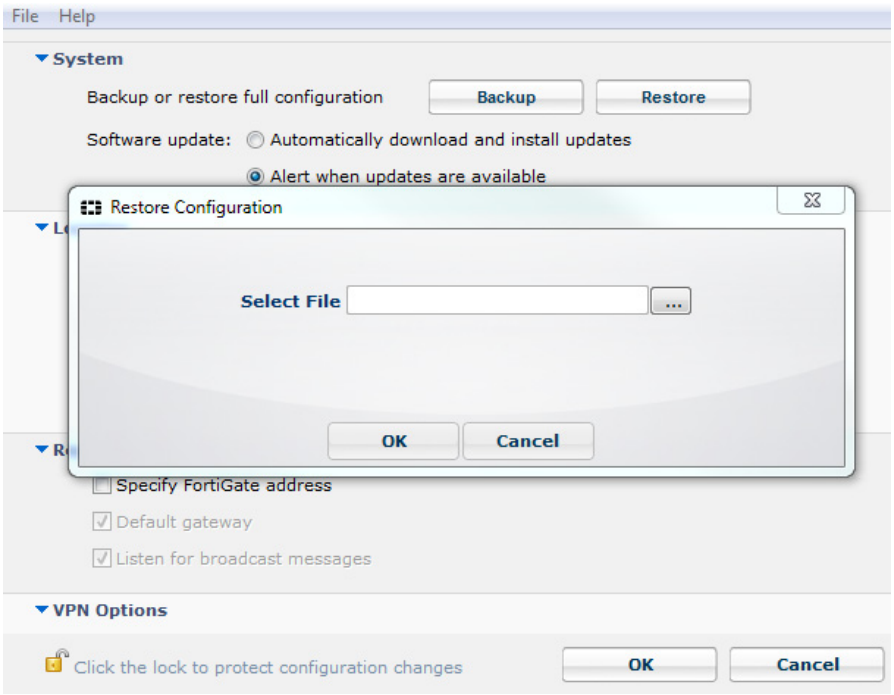
Figure 2: Backup configuration file options



Restore the full configuration file

To restore a full configuration file, select *File* on the toolbar, and *Settings* on the drop-down menu. Select *System* to view the drop-down menu. On this menu you can select *Restore* to import a backup of the full configuration file. Select *Restore* and browse for the file on your local hard disk drive.

Figure 3: Restore a configuration file



If the configuration was protected with a password, a password textbox will be displayed. Enter the password used to encrypt the backup configuration file.

Backup and restore command line utility commands and syntax

Fortinet provides administrators the ability to import and export configurations via the CLI. The fcconfig.exe utility can be run locally or remotely as the system user (or admin user) to import or export the configuration file. The fcconfig utility is located in the C:\Program Files (x86)\Fortinet\FortiClient> directory.

The following commands are available for use:

Backup the configuration file

```
FCConfig -m all -f <filename> -o export -i 1
```

Backup the configuration file (encrypted)

```
FCConfig -m all -f <filename> -o export -i 1 -p <encrypted password>
```

Restore the configuration file

```
FCConfig -m all -f <filename> -o import -i 1
```

Restore the configuration file (encrypted)

```
FCConfig -m all -f <filename> -o import -i 1 -p <encrypted password>
```

Export the VPN tunnel configuration

```
FCConfig -m vpn -f <filename> -o exportvpn -i 1
```

Export the VPN tunnel configuration (encrypted)

```
FCConfig -m vpn -f <filename> -o exportvpn -i 1 -p <encrypted
    password>
```

Import the VPN tunnel configuration

```
FCConfig -m vpn -f <filename> -o importvpn -i 1
```

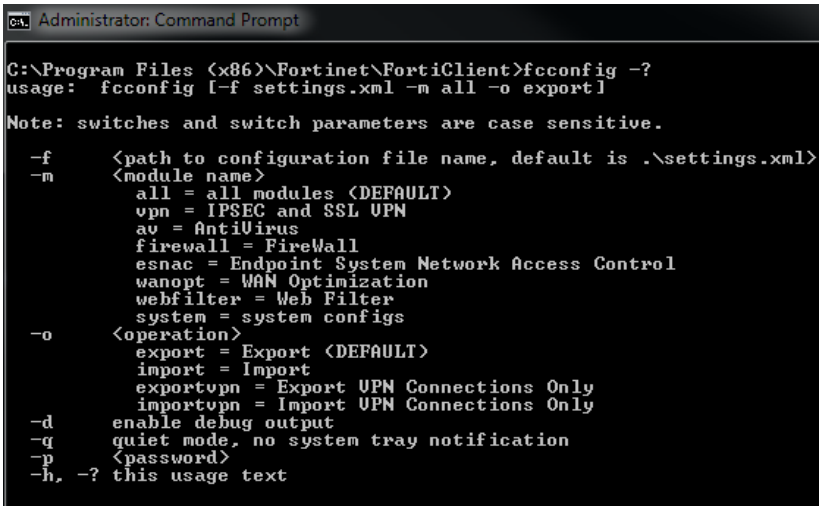
Import the VPN tunnel configuration (encrypted)

```
FCConfig -m vpn -f <filename> -o importvpn -i 1 -p <encrypted
    password>
```

Switches and switch parameters are case sensitive.

Backup and restore CLI commands are an advanced configuration option.

Figure 4: Administrative command prompt



The fcconfig utility will be updated for the next patch to include vulnerability scan and single sign-on mobility agent parameters.

The command `fccconfig -f settings.xml -m all -o export` will export the configuration as XML file in the FortiClient directory. See Figure 5 for an XML configuration example.

Figure 5: Exported XML configuration example

Upload the FortiClient XML file to FortiGate

In FortiOS v5.0.0 or later, the buffer size for the Endpoint Control XML configuration is 32KB.

Full configuration option

You need to enable advanced configuration from CLI to upload the FortiClient XML file. Enter the following command on the FortiGate:

```
config endpoint-control profile
  edit "default"
  config forticlient-winmac-settings
    set forticlient-advanced-cfg enable
    set forticlient-advanced-cfg-buffer "copy&paste your advanced
        forticlient xml configuration here"
    end
  next
end
```

After forticlient-advanced-cfg is enabled, forticlient-advanced-cfg-buffer setting is available from the CLI. You can also choose to copy/paste the XML content from the Web-based Manager, go to *Device* > *Endpoint Profile.*

Advanced VPN configuration

If you only want to upload the VPN configurations, you can use the CLI as well:

```
config endpoint-control profile
  edit "default"
  config forticlient-winmac-settings
    set forticlient-vpn-provisioning enable
    set forticlient-advanced-vpn enable
    set forticlient-advanced-vpn-buffer "copy&paste your advanced
        VPN configuration XML here"
    end
  next
end
```

Advanced Features

Advanced features (Windows)

Connect VPN before logon (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN will connect first, then logon to AD/Domain.

```
<forticlient_configuration>
  <vpn>
    <options>
      <show_vpn_before_logon>1</show_vpn_before_logon>
      <use_windows_credentials>1</use_windows_credentials>
    </options>
  </vpn>
</forticlient_configuration>
```

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
        <options>
        ...
        </options>
          <connections>
            <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
              <prompt_certificate>0</prompt_certificate>
              <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                   .143</server>
              <redundantsortmethod>1</redundantsortmethod>
              ...
          </ike_settings>
        </connection>
      </connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are committed.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0, and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first on the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
      </options>
      <connections>
        <connection>
          <name>ssl_90_1</name>
          <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
              3</server>
          ...
        </connection>
      </connections>
    </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are committed.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ipsecdemo.fortinet.com</autoconnect_tunnel>
```

Inside:

```
<vpn>
  <options>
```

Save password is also needed because it is autoconnect:

```
<save_password>1</save_password>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

Inside:

```
<vpn>
  <connection>
```

Advanced features (Mac OS X)

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
  <vpn>
    <ipsecvpn>
        <options>
        ...
        </options>
          <connections>
            <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
              <prompt_certificate>0</prompt_certificate>
              <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61
                  .143</server>
              <redundantsortmethod>1</redundantsortmethod>
              ...
          </ike_settings>
        </connection>
      </connections>
    </ipsecvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are committed.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0, and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first on the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
        ...
      </options>
      <connections>
        <connection>
          <name>ssl_90_1</name>
          <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:44
              3</server>
          ...
        </connection>
      </connections>
    </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are committed.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN auto connect uses the following XML tag:

```
<autoconnect_tunnel>ssl 198 no cert</autoconnect_tunnel>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

VPN before logon is currently not supported in FortiClient v5.0 Patch Release 1 (Mac OS X).

VPN tunnel & script (Microsoft Windows)

Feature overview

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They will be defined as part of a VPN tunnel configuration on FortiGate's XML format Endpoint Profile. The profile will be pushed down to FortiClient from FortiGate. When

FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed. These scripts can also be configured directly on FortiClient, by importing the XML configuration file.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>windows</os>
      <script>
        <script>
          <![CDATA[
net use x: \\192.168.10.3\ftpshare /user:Honey Boo Boo
md c:\test
copy x:\PDF\*.* c:\test
              ]]>
        </script>
      </script>
  </on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>windows</os>
    <script>
      <script>
        <![CDATA[
net use x: /DELETE
          ]]>
</script>
        </script>
    </script>
</on_disconnect>
```

VPN tunnel & script (Mac OS X)

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
  <script>
    <os>mac</os>
    <script>
      /bin/mkdir /Volumes/installers
      /sbin/ping -c 4 192.168.1.147 >
           /Users/admin/Desktop/dropbox/p.txt
      /sbin/mount -t smbfs
           //kimberly:RigUpTown@ssldemo.fortinet.com/installer
           s /Volumes/installers/ >
           /Users/admin/Desktop/dropbox/m.txt
      /bin/mkdir /Users/admin/Desktop/dropbox/dir
      /bin/cp /Volumes/installers/*.log
           /Users/admin/Desktop/dropbox/dir/.
    </script>
  </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
  <script>
    <os>mac</os>
    <script>
      /sbin/umount /Volumes/installers
      /bin/rm -fr /Users/admin/Desktop/dropbox/*
  </script>
  </script>
</on_disconnect>
```

Index

S

U

V

W

X